Universidade de Aveiro
2017

Departamento de Engenharia Civil

Manuela Alexandra Grilo Alves Borges

Gestão de Risco em Infraestruturas de Abastecimento de Água

Universidade de Aveiro
2017

Departamento de Engenharia Civil

Manuela Alexandra Grilo Alves Borges

Gestão de Risco em Infraestruturas de Abastecimento de Água

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Civil, realizada sob a orientação científica da Professora Doutora Maria Fernanda da Silva Rodrigues, Professora Auxiliar do Departamento de Engenharia Civil da Universidade de Aveiro e coorientação científica do Professor Doutor Hugo Filipe Pinheiro Rodrigues, Professor Adjunto da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Para a minha irmã, Andreia

o júri

presidente

Prof. Doutor Joaquim Miguel Gonçalves Macedo
professor auxiliar da Universidade de Aveiro

Doutora Sandra Marisa Silva Costa
investigadora da Faculdade de Engenharia da Universidade do Porto

Prof. Doutora Maria Fernanda da Silva Rodrigues
professora auxiliar da Universidade de Aveiro

agradecimentos

À minha orientadora, a Professora Doutora Maria Fernanda Rodrigues, um agradecimento pela disponibilidade sempre demonstrada, pelo interesse e apoio que sempre manifestou ao longo destes meses. Ao meu coorientador Professor Doutor Hugo Rodrigues pela igual disponibilidade e apoio.

Um agradecimento à empresa Águas da Região de Aveiro, em particular ao Engenheiro Alberto Roque, à Engenheira Elisabete Pinheiro, ao Técnico de SIG Vítor Maia e ao Responsável de Manutenção Mário Duarte pela disponibilização dos elementos da rede de abastecimento de água de Aveiro e pela disponibilidade e auxílio prestado.

Ao Hélder por todo o apoio incondicional e compreensão nos momentos mais difíceis deste percurso. Pelo amor e amizade, pelas palavras de motivação e pela paciência que sempre demonstrou.

Por último, à pessoa a quem dedico este trabalho, à minha irmã Andreia, que tornou esta experiência possível e me apoiou ao longo do meu percurso académico.

palavras-chave Gestão de risco, infraestruturas críticas, abastecimento de água, metodologias de avaliação de risco, ArcGIS, ArcMap.

resumo

As redes de abastecimento de água são infraestruturas críticas essenciais às funções vitais da sociedade, da saúde, da segurança e do bem-estar económico e social que devem ser mantidas e preservadas, de forma a assegurar o seu bom funcionamento. A adequada gestão dessas infraestruturas consiste num ponto fundamental para esse bom funcionamento.

Tendo em consideração a importância que infraestruturas críticas, como as redes de abastecimento de água, têm para o dia-à-dia de todos os setores da sociedade, devem ser analisados os riscos a que estão sujeitas e as consequências que podem advir desses riscos. Assim, é importante que as empresas que gerem esses ativos incorporem nas suas atividades a gestão de risco.

No âmbito da gestão de risco pretende-se com este trabalho identificar as vulnerabilidades das infraestruturas de abastecimento de água, através da análise dos riscos a que estão sujeitas e identificar as medidas que necessitam de ser implementadas ou reforçadas.

Nesta dissertação, começa-se por analisar que iniciativas existem que tornam a gestão de risco de infraestruturas críticas, como redes de abastecimento de água, um elemento imprescindível na gestão das empresas. Analisam-se as metodologias de avaliação de risco existentes com o objetivo de identificar as mais valias de cada uma.

Como caso de estudo utilizou-se a rede de abastecimento da cidade de Aveiro composta por 15 reservatórios, dos quais 5 são elevados e 10 são apoiados. Essa rede é analisada através do *ArcMap*, *software* do *ArcGIS desktop*, que permite um melhor entendimento do funcionamento do caso de estudo.

A gestão de risco é aplicada ao caso de estudo sendo determinada a probabilidade e possíveis consequências de seis categorias de ameaças distintas, em oito cenários, que permitem analisar os níveis de risco da rede através da elaboração de mapas de risco. Identificam-se ainda medidas a implementar de forma a melhorar a resposta a potenciais incidentes ou prevenir a sua ocorrência.

keywords Risk Management, critical infrastructures, water supply, risk assessment methodologies, ArcGIS, ArcMap

abstract

Water supply networks are critical infrastructures essentials to the vital functions of society, of health, safety and economic and social wellbeing which, must be maintained and preserved to ensure their proper functioning. The proper management of those infrastructures is a key point to ensure their proper functioning.

Considering the importance of critical infrastructures, such as water supply networks, for the daily life of all sectors of society, the risks to which they are exposed and the consequences of such risks must be analysed. Thus, it is important that companies that are responsible for the management of these assets incorporate risk management in their activities.

In the scope of risk management, this work intends to identify the vulnerabilities of water supply infrastructures, by analysing the risks they are exposed and to identify the measures that need to be implemented or reinforced.

This dissertation begins analysing what initiatives exist for risk management of critical infrastructures, such as water supply networks, considering this as an essential element in the management of companies. Risk assessment methodologies were analised to identify the vantages and disadvantages of each one. As a case study, it was used the supply network of Aveiro city, which is composed by 15 reservoirs, 5 elevated and 10 supported. This network was analyzed resourcing ArcMap, ArcGIS desktop software, which allows a better understanding of how the case study works.

Risk management was applied to the case study and the probability and possible consequences of six distinct categories of threats were determined in eight scenarios, allowing the analysis of the network's risk levels through the development of risk maps. Measures to improve the response or to prevent the occurrence of potential incidents were also identified.

Índice Geral

Índice de Figuras

Índice de Tabelas

Lista de abreviaturas, acrónimos e siglas

AdRA – Águas da Região de Aveiro

AMC – Associação de Municípios do Carvoeiro

ANL – Argonne National Laboratory

APFM – Associação Portuguesa de Facility Management

APSEI – Associação Portuguesa de Segurança

BIRR - Better Infrastructure Risk and Resilience

CARVER2 – Criticality, Accessibility, Recoverability, Vulnerability, Espyability and Redundancy

CIMPA – Critical Infrastructure Protection Modelling and Analysis

CIMS – Critical Infrastructure Modelling Simulation

CIP – Critical Infrastructure Protection

CIP/DSS - Critical Infrastructure Protection – Decision Support System

CMI – Consequence Measure Index

DEMA – Danish Emergency Management Agency

DHS – Department of Homeland Security

DU – Dias úteis

EPCIP – European Programme for Critical Infrastructure Protection

ESRI – Environmental Systems Research Institute

ETA – Estação de Tratamento de Água

EURACOM - European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks

EURAM - European Risk Assessment Methodology project

FAIT – Fast Analysis Infrastructure Tool

FM – Facility Management

FR – Fator de Risco

FS/F – Fins de semana/Feriados

FTA – Fault Tree Analysis

FEMA – Federal Emergency Management Agency

GNR – Guarda Nacional Republicana

HSPD-7 – Homeland Security Presidential Directive 7

ICE – Infraestrutura Crítica Europeia

IFMA – International Facility Management Association

INE – Instituto Nacional de Estatística

IPMA – Instituto Português do Mar e da Atmosfera

ISO – International Organization for Standardization

IST – Infrastructure Survey Toll

JRC – Joint Research Centre

LNEC – Laboratório Nacional de Engenharia Civil

MIN - Multilayer Infrastructure Network

MMC - Multi-Hazard Mitigation Council

NEMO – Net-Centric Effects-based Operations Model

NIPP – National Infrastructure Protection Plan

NISAC - National Infrastructure Simulation and Analysis Center

NSCI – National Strategy for Critical Infrastructure

NSRAM - Network Security Risk Assessment Modelling

OBR – Oliveira de Bairro

PMI - Protection Measure Index

PPS – Physical Protection System

PSP – Polícia de Segurança Pública

RAM – Risk Assessment Management

RMI - Resilience Measure Index

RVA - Risk and Vulnerability Analysis

SCADA - Supervisory Control and Data Acquisition

SFP – Seventh Framework Programme

SIG – Sistema Informação Geográfica

SRAM - Sandia Risk Assessment Methodology

SSA – Specific Sectorial Agency

TI – Tecnologia da Informação

UE – União Europeia

UNDP – United Nations Development Programme

US CIP – United States Critical Infrastructure Programme

VI - Vulnerability Index

ZA – Zona Alta

ZB – Zona Baixa

ZMC – Zona de Monitorização e Controlo

Capítulo 1

Introdução

Capítulo 1 - Introdução

1.1 Enquadramento Geral

1.2 Objetivos e Metodologia

1.3 Organização e Estrutura da Dissertação

1 Introdução

1.1 Enquadramento Geral

Nos últimos anos tem havido um aumento da consciencialização para o facto da fase de operação e manutenção das estruturas e infraestruturas existentes ser a fase que requer mais investimento por parte das entidades que exploram as infraestruturas. Assim, é necessário refletir sobre as estratégias para melhorar a gestão dessas estruturas e infraestruturas.

A avaliação e gestão de risco é fundamental, pois permite determinar os riscos a que uma estrutura ou infraestrutura está sujeita, avaliar a probabilidade de ocorrerem, a incidência que podem ter na estrutura ou infraestrutura, assim como no desempenho da sua função ou na sociedade, e os procedimentos e normas que se devem adotar em caso de qualquer ocorrência.

O sociólogo Ulrick Beck definiu a sociedade de hoje como sociedade de risco. Isto porque defendia que a sociedade se caracteriza pelo processo de globalização, encontrando-se em constante desenvolvimento tecnológico e promovendo a individualização. Torna-se assim, numa sociedade opaca e em constante mutação, o que resulta no aumento do grau de incerteza em relação a acontecimentos futuros (Oliveira, 2015).

Sociedade de risco distingue-se por se estar num mundo cada vez mais conflituoso, colocando novos desafios à segurança. Desafios esses que englobam violência urbana, criminalidade transnacional e novas formas de terrorismo. De forma a minimizar as consequências destes acontecimentos e outros, como catástrofes naturais, é necessário recorrer à gestão de riscos (Oliveira, 2015).

A gestão de riscos visa a antecipação de acontecimentos e, assim, diminuir a incerteza e as falhas no processo produtivo, sendo que o seu objetivo não é necessariamente diminuir ou eliminar os riscos, mas minimizar os efeitos adversos que podem resultar destes. Assim, define-se gestão de riscos como um processo de identificação de potenciais riscos, analisando o impacto que estes podem ter, determinando a probabilidade da sua ocorrência, de forma a criar medidas e políticas que garantam o equilíbrio entre riscos e custos (Rodrigues, 2013). O objetivo da gestão de riscos consiste na proteção dos recursos humanos, materiais, ambientais e financeiros (UNDP, 2010).

A gestão de risco é aplicada ao nível financeiro, na gestão de infraestruturas, no planeamento urbano, nas atividades industriais, entre outros. No caso da presente dissertação aborda-se a gestão de riscos em meio urbano e em infraestruturas de

abastecimento de água. Os riscos a que o meio urbano está sujeito afetam as infraestruturas que nele existem e, vice-versa. Por exemplo, explosões constituem um risco urbano e esse evento pode provocar danos em tubagens de redes públicas que constituem as respetivas infraestruturas. Por outro lado, a rotura de uma tubagem constitui um risco da infraestrutura, no entanto pode resultar na interrupção do abastecimento e, por consequência, em efeitos no meio urbano.

1.2 Objetivos e Metodologia

As redes urbanas de abastecimento de água são geralmente compostas por fontes de água, condutas adutoras, estações de tratamento e redes de abastecimento e estão expostas a uma variedade de riscos que ameaçam o bom funcionamento das mesmas (Roozebahani *et al.,* 2012). Sendo a água um bem essencial à sociedade, a análise, mitigação ou eliminação desses riscos devem ser consideradas uma prioridade.

Na presente dissertação pretende-se analisar potenciais riscos que infraestruturas de distribuição e armazenamento de água possam estar sujeitos, compreender como o acontecimento de um evento associado a determinado risco, afeta a rede de abastecimento de água e, por consequência, os utilizadores da mesma, e ponderar que medidas de proteção ou mitigação podem ser implementadas de forma a minimizar, as consequências resultantes de determinado evento. Assim, a presente dissertação tem como objetivo proceder à avaliação para posterior gestão de risco de uma rede de abastecimento de água, sendo o caso de estudo a rede de abastecimento de água do concelho de Aveiro, gerida pela AdRA – Águas da Região de Aveiro.

Com o intuito de alcançar os objetivos pretendidos seguiu-se a metodologia que se descreve de seguida. Numa primeira fase efetuou-se uma pesquisa exaustiva em relação à temática da gestão de risco, tanto de forma generalizada como aplicada às redes de abastecimento de água.

Na segunda fase, de forma a definir a metodologia a aplicar, realizou-se a análise de diversas metodologias de avaliação de risco, tendo em consideração critérios considerados importantes para a aplicação da mesma ao caso de estudo.

Numa terceira fase, procede-se à análise dos elementos do caso de estudo disponibilizados pela AdRA para identificar que informação adicional seria necessário obter. Esta informação foi então adicionada ao *ArcMap* para se analisar o funcionamento da rede de abastecimento em estudo.

Por último, aplicou-se a metodologia selecionada ao caso de estudo tendo em conta cenários e categorias de ameaças distintos. Nesta última fase, analisam-se os eventos provocados por cada um dos cenários e são identificadas medidas que podem ser implementadas de forma a minimizar as consequências de cada cenário.
Com o intuito de atingir o objetivo principal definido anteriormente, os objetivos secundários da presente dissertação são:

- Efetuar a revisão bibliográfica dos conceitos a serem abordados;
- Análise de metodologias de avaliação de risco;
- Analisar informações disponibilizadas relativamente ao caso de estudo e identificar informação adicional a recolher;
- Adicionar informação recolhida ao *ArcMap*;
- Proceder à gestão de risco do caso de estudo;
- Concluir sobre os resultados obtidos neste processo.

1.3 Organização e Estrutura da Dissertação

A presente dissertação está dividida em quatro capítulos. O primeiro capítulo enquadra a dissertação desenvolvida e define os principais objetivos e metodologia aplicada, bem como a forma como esta se encontra organizada.
O segundo capítulo reflete a revisão bibliográfica realizada, na qual é apresentado o enquadramento da gestão de risco e o seu papel no *Facility Management* (FM). Aborda-se ainda as iniciativas de proteção de infraestruturas e metodologias de avaliação de risco existentes. Por fim, identifica-se a metodologia a aplicar na presente dissertação.
No terceiro capítulo, descreve-se o caso de estudo e o *software* utilizado para esclarecer o funcionamento da rede de abastecimento e mapear os riscos da mesma para cada cenário desenvolvido. Esses cenários resultam da gestão de risco realizada também neste capítulo.
No quarto e último capítulo, são apresentadas considerações finais e indicam-se futuros trabalhos complementares a desenvolver neste domínio de investigação.

Capítulo 2

Gestão de Risco

Capítulo 2 – Gestão de Risco

2 Gestão de Risco

2.1 Enquadramento Geral

O desafio de uma gestão segura das infraestruturas dos países continua a ser uma área de preocupação tanto para os governos como para os proprietários e operadores de infraestruturas críticas (Pye *et al.,* 2006).

Os sistema e instalações de infraestruturas críticas estão sujeitos a vários modos de falha diferentes. Assim, é importante antecipar os modos possíveis, a probabilidade da sua ocorrência e a gravidade dessas consequências (Baker *et al.,* 2003). Os perigos a que as infraestruturas críticas estão sujeitas podem ser intencionais, p.e. terrorismo, sabotagem, ataques cibernéticos, entre outras; ou não intencionais, como acidentes, envelhecimento, catástrofes naturais, etc. Perigo define-se como um elemento que por si só ou em combinação com outros, tem o potencial intrínseco de originar um risco. Uma situação que represente um nível de ameaça à vida, saúde, propriedade ou ambiente corresponde a um perigo (Vasyl *et al.*, 2013).

A norma ISO31000 – Gestão de Risco, define risco como o efeito da incerteza sobre os objetivos, em que um efeito é um desvio do esperado, positivo e/ou negativo. A norma assume que os objetivos podem ter diferentes aspetos, tais como metas financeiras, de saúde, segurança e ambientais, e que podem ser aplicados a diferentes níveis: estratégico, organizacional, projeto, produto e processo. Quando se realiza a gestão de risco, pode escolher-se entre, por exemplo, reduzir o risco ou implementar ações de proteção.

A forma mais eficaz de examinar os benefícios entre reduzir o risco e os custos da implementação de ações de proteção é utilizar um sistema de apoio à decisão que incorpore informações sobre ameaças, avaliações de vulnerabilidade e consequências de interrupção através de modelação e simulação avançadas (Bush *et al.,* 2005). Vulnerabilidade é a manifestação dos estados inerentes ao sistema que podem ser explorados para afetar adversamente esse sistema (Haimes, 2006). O projeto ESPON *Hazards* define vulnerabilidade como a combinação de potencial de dano e capacidade de resposta, considerando ainda a sua versatilidade ao reconhecer três dimensões de vulnerabilidade: económica, social e ecológica (Kumpulainen, 2006).

No mundo de hoje, diferentes redes de infraestruturas, p.e. transporte, energia, água, comunicações, estão altamente interligadas. Essa interligação faz com que as mudanças nas capacidades de uma rede sejam sentidas em outras redes. Essas dependências não se limitam à localização do incidente original que causa a mudança, e os efeitos resultantes

são muitas vezes adversos e duradouros. Mudanças localizadas em uma rede muitas vezes terão efeitos regionais e algumas vezes globais em outros domínios (Goodwin *et al.*, 2005). As interdependências entre infraestruturas e a resiliência das mesmas, retorno rápido para a função completa após a ocorrência de eventos indesejados, são dois aspetos importantes na gestão de infraestruturas críticas.

Nos pontos seguintes são identificadas iniciativas de Proteção de Infraestruturas Críticas existentes na Europa, nos Estados Unidos da América e no Canadá e descritas várias metodologias de avaliação de riscos, com o objetivo de identificar as vantagens e desvantagens de cada uma, de forma a desenvolver uma metodologia de avaliação de riscos que permita a melhor gestão de riscos do caso de estudo da presente dissertação.

2.2 Facility Management

No ambiente económico-financeiro atual as oportunidades de negócios e a sua execução estão constantemente interligadas a recursos monetários. A necessidade de identificar, avaliar, gerir e monitorizar tornou-se num assunto crítico para atingir a sustentabilidade. Consequentemente, adotar uma abordagem estratégica no que respeita ao FM tornou-se uma atividade chave e uma norma nas organizações (Saleh *et al.*, 2011).

A Associação Portuguesa de *Facility Management (*APFM) define FM "*como a gestão integrada dos locais e ambientes de trabalho, com o objetivo de otimizar os espaços, os processos e as tecnologias envolventes em prol das pessoas e das organizações*" (APFM, 2017).

Segundo a *International Facility Management Association (IFMA),* "*FM é uma profissão que abrange várias disciplinas para garantir a funcionalidade do ambiente construído, através da integração de pessoas, lugar, processo e tecnologia*" (IFMA, 2017).

A aplicação do FM à indústria da construção é relativamente recente, isto porque antigamente acreditava-se que o maior investimento necessário durante o ciclo de vida de uma estrutura era feito na fase de construção. Contudo, existem dados que indicam que a fase de projeto e construção corresponde apenas a aproximadamente 20% do valor total da estrutura, enquanto que aproximadamente 80% dos custos ocorrem na fase de operação e manutenção (Silva, 2003).

Nos últimos anos, a aplicação de técnicas e abordagens de gestão de risco, em todas as indústrias, tem vindo a ser cada vez mais reconhecida como um elemento-chave duma estrutura de gestão e administração eficaz (FMA, 2004).

O planeamento e realização de gestões de risco eficazes são um componente essencial para a aplicação do FM. O setor do FM está a evoluir de uma atividade principalmente organizacional para uma abordagem estratégica abrangente que influencia o planeamento e o desempenho organizacional. Esse desenvolvimento resulta numa forma diferente de pensar no FM que tem muito em comum com a temática emergente da gestão de risco (FMA, 2004).

A gestão de risco deve ser englobada no FM de infraestruturas importantes de forma a melhorar a preparação das mesmas a potenciais riscos e assim, diminuir ou mitigar as consequências dos mesmos.

2.3 Iniciativas de Proteção de Infraestruturas Críticas

2.3.1 Programa Europeu para Proteção de Infraestruturas Críticas

O *European Programme for Critical Infrastructures Protection* (EPCIP) consiste num plano que engloba várias ferramentas, ilustradas na

Figura 1, que permitem proteger infraestruturas críticas europeias.

Figura 1 - Ferramentas para Proteção de Infraestruturas Críticas na Europa (Giannopoulos *et al.*, 2012)

A Diretiva 2008/114/EC, de 8 de dezembro de 2008 é a ferramenta legislativa do programa *Critical Infrastructure Protection* (CIP) onde são considerados apenas os sectores de energia (eletricidade, gás e petróleo), e transportes. *"O artigo 3.o impõe aos*

Estados-Membros a obrigação de identificarem as infraestruturas críticas suscetíveis de serem designadas como Infraestruturas Críticas Europeias (ICE)", sendo ICE, de acordo com a alínea b), do artigo 2º, "*a infraestrutura crítica situada nos Estados-Membros cuja perturbação ou destruição teria um impacto significativo em pelo menos dois Estados-Membros".* O processo de identificação e designação das infraestruturas críticas na Europa consiste em quatro fases, identificadas na diretiva 2008/14/EC. As fases são as seguintes:

- **Fase 1:** Cada Estado-Membro aplica critérios sectoriais para efetuar uma primeira seleção das infraestruturas críticas dentro de um determinado sector;
- **Fase 2:** Cada Estado-Membro aplica a definição de «infraestrutura crítica» constante da alínea a) do artigo 2.o às potenciais ICE identificadas na Fase 1. A definição, de acordo com o artigo mencionado, de infraestrutura crítica: "*o elemento, sistema ou parte deste situado nos Estados-Membros que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo num Estado-Membro, dada a impossibilidade de continuar a assegurar essas funções".*
- **Fase 3:** Cada Estado-Membro aplica o elemento transfronteiriço da definição de ICE constante da alínea do artigo 2.º b) às potenciais ICE que tenham concluído as duas primeiras fases do procedimento. As potenciais ICE que correspondam à definição transitarão para a fase seguinte do procedimento. Para as infraestruturas que fornecem um serviço essencial, serão tidas em linha de conta as alternativas disponíveis e a duração da perturbação/recuperação.
- **Fase 4:** Cada Estado-Membro aplica critérios transversais às potenciais ICE remanescentes. Os critérios transversais têm em conta a gravidade do impacto e, no caso das infraestruturas que fornecem um serviço essencial, as alternativas disponíveis e a duração da perturbação/recuperação. As potenciais ICE que não preencham os critérios transversais não serão consideradas ICE.

As infraestruturas críticas europeias que tenham concluído todos os passos são dadas a conhecer apenas aos Estados-Membros que por elas possam ser afetados de forma significativa.

A diretiva 2008/114/EC encontra-se em revisão, de forma a serem discutidos os processos de identificação e designação e o âmbito da diretiva, tendo em conta a evolução contínua das infraestruturas críticas. Essa evolução levou a sistemas de infraestruturas mais complexos, com interação com camadas cibernéticas e físicas, em que as fronteiras dos sectores não estão claramente definidas.

2.3.2 *United States Critical Infrastructures Protection* (US CIP)

A *Homeland Security Presidential Directive* (HSPD-7) estabelece uma Lei americana para melhorar a proteção das infraestruturas críticas dos Estados Unidos, introduzindo uma estrutura, dirigida aos parceiros do Departamento de Segurança Interna (DHS) que permite identificar, priorizar e proteger as infraestruturas críticas das suas comunidades de ataques terroristas (DHS, 2017).

A diretiva HSPD-7 designa uma Agência Sectorial Específica (SSA) federal, para cada um dos sectores de infraestruturas críticas identificados, que lidera programas e atividades de proteção e resiliência. Esta diretiva permite ao DHS identificar falhas nos setores existentes e criar novos setores para preencher essas falhas. Os sectores identificados na diretiva são os seguintes (Caldwell, 2009):

- Sector de Agricultura e Alimentação;
- Sector Bancário e Financeiro;
- Sector Químico;
- Sector de Instalações Comerciais;
- Sector de Reatores Nucleares Comerciais, Materiais e Resíduos;
- Sector de Comunicações;
- Setor de Barragens;
- Setor de Base Industrial de Defesa;
- Setor de Sistemas de Tratamento de Água e Água Potável;
- Sector de Energia;
- Setor de Serviços de Emergência;
- Setor de Instituições Governamentais;
- Setor de Tecnologia de Informação;
- Setor de Monumentos e Ícones Nacionais;
- Setor de Correspondência e Distribuição;
- Setor de Saúde Pública e Cuidados de Saúde;

- Setor de Sistemas de Transporte;
- Setor de Fabrico (adicionado em 2008).

Comparando a abordagem do DHS com a abordagem Europeia, EPCIP é possível concluir que ambas apresentam abordagens sectoriais, no entanto as abordagens diferem em dois pontos. Ao contrário da EPCIP a HSPD-7 foca-se na resiliência, e a EPCIP contém um procedimento formal para identificar e designar as infraestruturas críticas não considerado na HSPD-7.

A estrutura de implementação do US CIP é o programa *National Infrastructure Protection Plan* descrito no ponto 2.3.2, que integra os esforços em relação às medidas de proteção das infraestruturas críticas dos vários sectores, define as obrigações e responsabilidades das várias entidades a nível estatal e federal, estabelece ainda, a estrutura para a gestão de riscos de infraestruturas críticas.

2.3.3 Estratégia Nacional e Plano de Ação para Proteção de Infraestruturas Críticas do Canadá

National Strategy for Critical Infrastructure Protection estabelece uma estrutura para reforçar a resiliência das infraestruturas críticas, sendo a resiliência o objetivo final pretendido. Este objetivo é alcançado através de um plano, elemento de execução da estratégia nacional, que estabelece as ações na área da organização de parcerias, implementação de uma abordagem de gestão de todos os riscos e da partilha de informação.

A distribuição das responsabilidades entre os protagonistas, ou seja, os governos federal e providencial/territorial, e operadores das infraestruturas críticas, é um ponto interessante do plano de ação canadiano. Para além de promover uma abordagem multicamada que requer a colaboração dos vários protagonistas, essa distribuição demonstra que a resiliência é abordada nos níveis territorial e governamental, enquanto que os operadores são responsáveis pela identificação, gestão e mitigação dos riscos associados ao seu ambiente.

Uma justificação para a distribuição de responsabilidades aplicada ao plano de ação encontra-se no facto de que a resiliência não pode ser abordada ao nível dos ativos/operadores, visto que requer a colaboração de várias entidades, por vezes de sectores diferentes (Giannopoulos *et al.*, 2012).

2.4 Estado de Arte de Metodologias de Avaliação de Riscos na UE e no mundo

Existe um grande número de metodologias de avaliação de riscos baseadas, na sua maioria, numa abordagem comum e linear que consiste nos seguintes elementos principais (Giannopoulos *et al.*, 2012):

- Identificação e classificação de ameaças;
- Identificação de vulnerabilidades;
- Avaliação do impacto.

Atualmente, é necessário definir uma metodologia que além de determinar os elementos principais mencionados, tenha em conta os utilizadores alvo da metodologia, as interdependências entre infraestruturas críticas de diferentes sectores e a análise ao nível de infraestruturas/sistemas e ao nível de sistemas de sistemas.

Na descrição de cada metodologia serão analisados determinados critérios que se consideram fundamentais para a gestão de riscos de um sistema de infraestruturas, sendo assim possível realizar uma comparação entres as diferentes metodologias.

Os critérios que serão considerados para cada metodologia são o âmbito, os objetivos, as técnicas e padrões aplicados, a consideração de interdependências (físicas, cibernéticas, geográficas ou lógicas) e da resiliência, os perigos considerados (naturais ou humanos), o domínio em que se aplica (ativos, nível da infraestrutura/sistema ou nível de sistemas de sistemas) e, por fim, a quem se destina (legisladores, decisores, institutos de investigação) (Giannopoulos *et al.*, 2012).

2.4.1 *Better Infrastructure Risk and Resilience* (BIRR)

O Laboratório Nacional de Argonne (ANL) situado nos Estados Unidos, de forma a apoiar o DHS do mesmo país, procedeu ao desenvolvimento de metodologias que têm como objetivo avaliar os riscos e a resiliência de infraestruturas críticas quando sujeitas a catástrofes naturais ou perigos de origem humana.

O *Enhance Critical Infrastructure Protection* (ECIP) consiste no programa responsável pelo desenvolvimento das metodologias em dezoito sectores de infraestruturas críticas, indicados no ponto 2.3.2. O objetivo destas metodologias é proporcionar ferramentas a legisladores, decisores e operadores, que ajudem na análise de vários sectores, na identificação de vulnerabilidades e preparação de relatórios de risco.

O pilar da metodologia BIRR é a recolha de informação fidedigna, através de um questionário direcionado, o *Infrastructure Survey Tool* (Ferramenta de Levantamento de

Infraestruturas), desenvolvido pelo DHS e os seus assessores de proteção da segurança. A metodologia BIRR enfatiza ameaças terroristas ao nível dos ativos (Giannopoulos *et al.*, 2012). O diagrama *bowtie* (*bowtie diagram*) de gestão de risco, ilustrado na Figura 2, representa a forma como as ameaças, vulnerabilidades, consequências e resiliência se encaixam num processo de gestão de risco (Petit *et al.*, 2013).

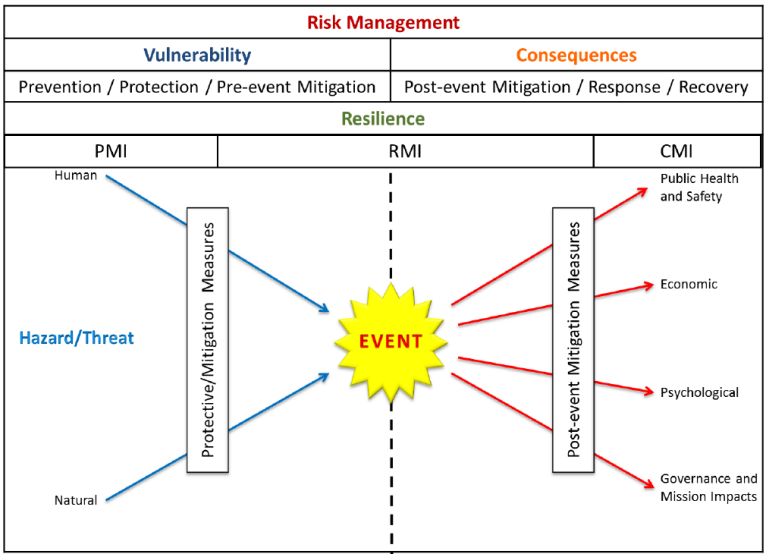


Figura 2 - Diagrama *bowtie* de Gestão de Risco (Petit *et al.*, 2013)

A coleta de informação permite quantificar os índices: índice de medidas de proteção (*Protection Measure Index, PMI*), índice de vulnerabilidade (*Vulnerability Index, VI*), índice de medição da resiliência (*Resilience Measure Index, RMI*) e índice de medição de consequências (*Consequences Measure Index, CMI*) (Petit *et al.*, 2013).

O principal objetivo é analisar o desempenho de uma instalação em termos de proteção/vulnerabilidade, resiliência, consequência e, por fim, risco. Sendo depois possível propor opções para melhorar esse desempenho.

O *PMI*, que se centra na zona esquerda do diagrama da Figura 2, tem como objetivo desenvolver um indicador de desempenho chave que possibilite a caracterização da postura protetora de uma instalação e, de seguida, apoiar as decisões dos proprietários e operadores de infraestruturas críticas, permitindo a comparação entre infraestruturas semelhantes. A versão lançada em 2013 deste índice aborda elementos que caracterizam a segurança física, a gestão de segurança, força de segurança, partilha de informação e o histórico de atividades de segurança. Esse índice permite ainda calcular o *VI* que corresponde ao inverso do *PMI*, ou seja, se o *PMI* for elevado o *VI* é baixo, e vice-versa.

O *PMI* é calculado através da equação (2.1), em que d_i corresponde à constante de escala (peso, valor entre 0 e 1) que indica a importância relativa do componente i (i = 1, 2, 3, 4, 5) de medidas de proteção; e W_i corresponde ao valor do índice do componente i de medidas de proteção (isto é, segurança física, gestão de segurança, força de segurança, partilha de informações e histórico de atividade de segurança). O *VI* determina-se através da equação (2.2) (Petit *et al.*, 2013).

$$PMI = \sum_{i=1}^{5} d_i * W_i \tag{2.1}$$

$$VI = 100 - PMI \tag{2.2}$$

O *RMI* encontra-se no centro do diagrama da Figura 2, sendo que aborda elementos que caracterizam a preparação, medidas de mitigação, capacidade de resposta e mecanismos de recuperação. Por fim, o *CMI*, que se foca no lado direito do diagrama da Figura 2, caracteriza as consequências máximas potencialmente geradas por um evento adverso, numa instalação. Este índice inclui informações relativas à saúde pública e os impactos de segurança, económicos, psicológicos, na governança e na perda da instalação (Petit *et al.*, 2013).

O *PMI* é baseado na análise de decisão e *Multi-Attribute Utility Theory* (MAUT), teoria da utilidade de múltiplos atributos. Cada atributo que contribuí para a proteção da instalação é dividido em seus subcomponentes individuais, que são então organizados em quatro níveis de informação. A Figura 3 representa a estrutura dos componentes do nível 1 e subcomponentes dos níveis 2 e 3 do *PMI* (Petit *et al.*, 2013).

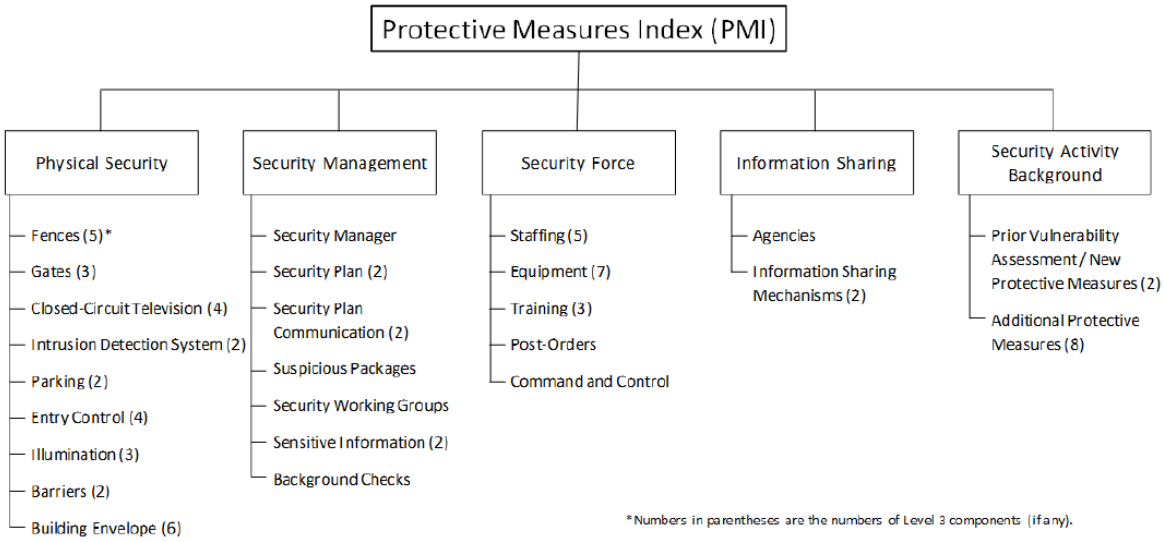


Figura 3 - Estrutura dos componentes e subcomponentes do *PMI* (Petit *et al.*, 2013)

No passo seguinte, especialistas definem a classificação e a importância relativa de vários cenários associados a cada subcomponente. Por exemplo, no caso do plano de segurança, incluído na gestão de segurança, os especialistas definem a classificação e a importância relativa para cada um dos seguintes exercícios: *tabletop*[1] com respondedores externos, *tabletop* sem respondedores externos, funcional com respondedores externos, funcional sem respondedores externos, em larga escala com respondedores externos, em larga escala sem respondedores externos e análise pós exercício/evento. Os valores atribuídos encontram-se na Tabela 1.

[1] Exercício *tabletop* - simula uma situação de emergência num ambiente informal e sem stress. Os participantes, geralmente constituídos por pessoal de nível de decisão e respondedores, se reúnem para discutir procedimentos simulados e problemas / soluções gerais no contexto de um cenário de emergência. O foco está no treino e familiarização com papéis, procedimentos e responsabilidades relativos à sinopse de emergência e injeções potenciais.

Tabela 1 - Valores da classificação e importância relativa (Petit *et al.*, 2013)

Type of Exercise	Team 1		Team 2		Team 3	
	Rank	Relative Importance	Rank	Relative Importance	Rank	Relative Importance
Tabletop (practical or simulated exercise)—does not include external responders.	7	20	7	40	6	60
Tabletop—includes external responders.	6	30	5	50	5	65
Functional (walk-through or specialized exercise)—does not include external responders.	5	50	5	50	4	75
Functional—includes external responders.	4	60	4	60	2	95
Full-scale (simulated or actual event)—does not include external responders.	2	80	2	80	3	90
Full-scale—includes external responders.	1	100	1	100	1	100
Exercise or actual event results are documented; corrective actions are identified and reported to executive management.	2	80	2	80	7	30

Tabela 2 - Valores da classificação e importância relativa (médias) (Petit *et al.*, 2013)

Type of Exercise	Rank	Relative Importance
Tabletop (practical or simulated exercise)—does not include external responders.	7	38.3
Tabletop—includes external responders.	6	46.9
Functional (walk-through or specialized exercise)—does not include external responders.	5	57.2
Functional—includes external responders.	4	70.1
Full-scale (simulated or actual event)—does not include external responders.	2	82.9
Full-scale—includes external responders.	1	100
Exercise or actual event results are documented; corrective actions are identified and reported to executive management.	3	74.3

Os valores de importância relativa global não são uma média direta dos valores definidos pelos especialistas pois os valores integram o ranking e, em seguida, a importância relativa de cada elemento. Por exemplo, o valor 74,3 da Tabela 2, seria 63,3 se fosse calculado através de uma média aritmética, no entanto tem-se em consideração que duas das equipas escolheram o exercício associado ao valor 74,3 como o segundo mais importante. Por fim, calcula-se o peso através de multiplicações cruzadas, tendo em conta que a soma dos vários pesos dos exercícios tem que dar um total de um. Não esquecer que alguns exercícios são mutuamente exclusivos, ou seja, um exercício funcional não será executado com e sem respondedores. Este processo é repetido para um dos subcomponentes (Petit *et al.*, 2013).

2.4.2 Proteção de Infraestruturas Críticas – Diretriz do Conceito de Proteção (PIC/DCP)

O Ministério Federal do Interior, o Gabinete Federal de Proteção Civil e da Resposta a Desastres e o Gabinete de Polícia Criminal Federal, entidades Alemãs, desenvolveram uma Diretriz do Plano de Proteção. Este, consiste num plano completo de proteção que acentua a importância das empresas privadas, sendo considerado mais do que uma metodologia de avaliação de riscos.

A metodologia desenvolvida pelas entidades alemãs tem como âmbito identificar diversas ameaças, desde desastres naturais a terrorismo e atos criminosos. Após a identificação dos riscos elabora recomendações em relação aos pontos vulneráveis e à gestão de riscos e desenvolve medidas de proteção para a infraestrutura.

O objetivo da metodologia é a cooperação entre o estado e as entidades operadoras das infraestruturas críticas, assegurando assim o bom funcionamento de infraestruturas importantes para a sociedade.

As interdependências são consideradas como efeitos secundários, que estão relacionados com o nível de dependência da infraestrutura em relação a um evento que não se desenvolve no interior da arquitetura desta infraestrutura. Assim, é necessário verificar se esse efeito ameaça a infraestrutura e, caso ameace, determinar através de que tipo de dependência. Um exemplo desta situação são as catástrofes naturais, em que a ameaça não é diretamente à infraestrutura crítica, mas podem constituir uma ameaça devido à dependência geográfica.

As empresas com negócio no domínio das infraestruturas críticas, de qualquer sector, são os utilizadores alvo desta metodologia. A resiliência não é abordada nesta metodologia (Giannopoulos *et al.*, 2012).

2.4.3 CARVER2

CARVER2, *Criticality Accessibility Recoverability Vulnerability Espyability Redundancy,* (Criticidade Acessibilidade, Recuperabilidade, Vulnerabilidade, Propensão para Espionagem, Redundância) consiste num método não técnico que permite comparar e classificar infraestruturas críticas e recursos chave. Esta metodologia tem em consideração desastres naturais e perigos de origem humana e destina-se a servir as necessidades de análise de infraestruturas do ponto de vista dos legisladores.

A implementação desta metodologia é feita através de uma ferramenta informática, ilustrada na Figura 4.

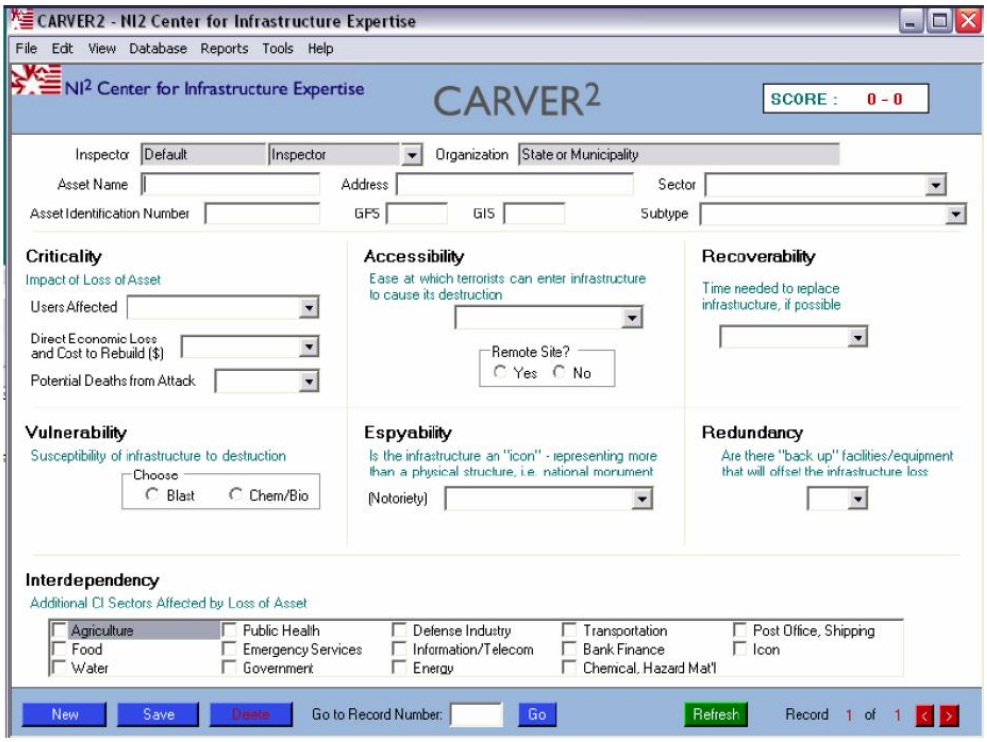


Figura 4 - Ferramenta de Implementação - CARVER2 (Giannopoulos *et al.*, 2012)

Nesta metodologia são abordados sete critérios:

- **Criticidade** – avaliação do impacto (está de acordo com as categorias de impacto consideradas na ECIP - utilizadores afetados, perda económica direta, custo de reconstrução e potenciais vítimas);
- **Acessibilidade** – avaliação da vulnerabilidade em termos de segurança física (possibilidade da entrada de terroristas com a intenção de provocar destruição);
- **Recuperabilidade** – cobre parcialmente a resiliência, tendo em conta que se refere à capacidade de recuperação da infraestrutura;
- **Vulnerabilidade** – cobre parte das potenciais vulnerabilidades da infraestrutura, como terrorismo, com ênfase em explosões e ameaças químicas e biológicas;
- **Propensão para Espionagem** – refere-se à função de uma infraestrutura como um ícone (por exemplo, local cultural);
- **Redundância** – refere-se à existência de infraestruturas de reserva que possam compensar a perda da infraestrutura em estudo;

- **Interdependências** – refere-se a sectores que são afetados pela perda ou interrupção do funcionamento da infraestrutura em estudo.

Apesar das interdependências serem abordadas entre sectores, não é a clara a forma como estas foram consideradas (as ligações entre ativos de diferentes sectores foram previamente definidas) nem o tipo de interdependências que se tem em conta. A ferramenta utilizada na implementação desta metodologia produz relatórios e uma pontuação para a classificação do ativo. Essa pontuação fornece uma medida intersectorial que permite a avaliação da importância de diferentes infraestruturas.
A metodologia descrita aborda vários critérios importantes, em simultâneo, ao nível dos ativos, no entanto seria interessante ajustar esta metodologia de forma a ser aplicada a níveis mais elevados, como sistemas de infraestruturas críticas (Giannopoulos *et al.*, 2012).

2.4.4 Simulação de Modelação de Infraestruturas Críticas (CIMS)

A metodologia CIMS tem como objetivo fornecer uma ferramenta a legisladores e, principalmente, a decisores, que permita tomar decisões rápidas na resposta a ameaças e, particularmente a desastres naturais. Esta ferramenta foi criada pelo Laboratório Nacional de Idaho, situado nos Estados Unidos, com a intenção de ser utilizada ao nível de cidades e países, tendo em conta todos os perigos, naturais e humanos, de forma a priorizar a resposta de emergência, com base no número de pessoas afetadas.
A construção dos modelos é feita através de mapas simples ou imagens aéreas, não sendo necessários dados detalhados de engenharia, que resulta num desenvolvimento rápido de um modelo simples, assim como a fácil atualização do mesmo, em tempo real, com base na informação disponível ao longo do evento.
Uma característica importante da ferramenta descrita é a capacidade de retratar a interoperabilidade de vários sistemas de infraestruturas, possibilitando, em caso de um evento destrutivo, captar a dinâmica das interdependências e a maneira como isso influência as equipas de emergência.
A resiliência da infraestrutura não é abordada, no entanto é mencionada a resiliência da sociedade através de medidas de emergência (Gionnapolous *et al.*, 2012).

2.4.5 Sistema de Apoio à Decisão de Proteção de Infraestruturas Críticas (CIP/DSS)

Os Laboratórios Nacionais de Argonne, Sandia e Los Alamos, situados nos Estados Unidos, desenvolveram a CIP/DSS, ferramenta de avaliação de risco que considera a probabilidade de ameaças ocorrerem, vulnerabilidades e impacto para todos os perigos, naturais e humanos, em vários tipos de infraestruturas (Giannopoulos *et al.*, 2012).

O programa CIP foi desenvolvido com três objetivos principais:

1. Desenvolver, implementar e evolver uma abordagem racional, que priorize estratégias e alocações de recursos do CIP, utilizando modelação, simulação e análise, de forma a avaliar vulnerabilidades, consequências e riscos;
2. Apresentar e avaliar propostas e opções de proteção, mitigação, resposta e recuperação;
3. Oferecer apoio, em tempo real, a decisores, durante crises e emergências.

Os utilizadores alvo desta metodologia são decisores e entidades governamentais que necessitam definir medidas de mitigação, táticas operacionais e priorizar recursos para a proteção de infraestruturas críticas. Esta metodologia é aplicada a altos níveis de sistemas de infraestruturas, por exemplo, a nível nacional.

Na metodologia CIP/DSS realiza-se a simulação de um evento admitindo incertezas nao *input*, tais como ameaças ou vulnerabilidades, obtendo-se assim uma estimativa do impacto do evento no *output* (Bush *et al.*, 2005). A Figura 5 representa a relação existente entre os decisores, as decisões e o CIP/DSS.

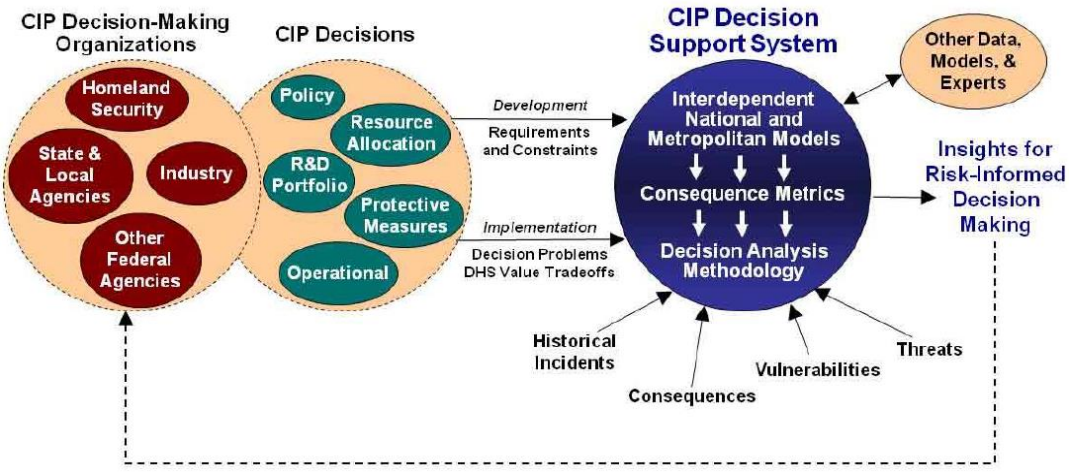


Figura 5 – Relação entre decisores, decisões e CIP/DSS (Bush *et al.*, 2005)

As interdependências são abordadas entre os sectores os 18 sectores, enumerados no ponto 2.3.2. O sistema de apoio à decisão incluí modelos de consequência, isto é, modelos que simulam a dinâmica das infraestruturas individuais e infraestruturas entre si, de acordo com as suas interdependências (Bush *et al.,* 2005).

O CIP/DSS-DM é um *software* desenvolvido no âmbito desta metodologia que auxilia em análises de equilíbrio complexas representadas pelos resultados de cenários de simulação, gerados em casos de estudo pelos modelos de consequência do CIP/DSS. Os resultados de cenários de simulação incluem consequências multidimensionais (impactos) que dependem de vários tipos de resposta a um possível evento. Os impactos podem ser quantificados em termos de fatalidades, lesões não fatais, doenças não fatais, perdas económicas, impactos na confiança pública e custos de implementação estratégias de mitigação.

A comparação entre medidas de mitigação é um processo importante para a proteção de infraestruturas críticas, no entanto é também um processo complexo. A ferramenta CIP/DSS-DM facilita este tipo de comparações pois fornece uma estrutura de visualização que combina várias medidas de custo e impacto em uma medida de mérito, que é uma métrica de preferência relativa, baseada na estrutura do valor do decisor (Samsa *et al.,* 2008).

Um ponto interessante da ferramenta CIP/DSS-DM é o facto de que caracteriza os decisores, ou seja, tendo em conta que a análise não é totalmente objetiva e que os pontos de vista das entidades envolvidas dependem da sua experiência, das suas crenças e valores, o *software* permite desenvolver perfis de decisores, tendo em conta os fatores que cada interveniente considera mais importantes e a sua atitude relativamente ao risco. De forma a elaborar o seu perfil, cada decisor atribui um valor a cada um dos elementos que quantificam os impactos, demonstrando assim a importância que cada elemento tem. Para facilitar, analisa-se a Tabela 3.

Tabela 3 - Exemplo de Estruturas de Valores de Decisores (Samsa *et al.*, 2008)

Impact Variable	Decision-Maker Value Structures		
	1	**2**	**3**
Cost of mitigation measures ($M)	1	1	40
Public confidence (PC point)	50	0	10
Human health and safety			
Fatalities (persons)	20	50	60
Nonfatal injuries (persons)	0.2	2	20
Nonfatal illnesses (persons)	0.2	2	10
Economic losses ($M)	1	1	60

O decisor 1 atribui os valores 1 milhão ao custo das medidas de mitigação e às perdas económicas assim, ao atribuir 50 valores à descida de um ponto na confiança pública, numa escala de 1 a 9, está a considerar que essa descida equivale a 50 milhões gastos em medidas de mitigação ou 50 milhões de perda económica.

O decisor 2 atribuiu os mesmos valores que o decisor 1 ao custo das medidas de mitigação e às perdas económicas. Ao impor 0 à descida da confiança pública, o decisor 2 considera que essa descida não tem qualquer influência na sua escolha de estratégias de mitigação. No caso das fatalidades, a atribuição de 50 valores, significa que cada fatalidade corresponde a 50 milhões gastos em medidas de mitigação ou 50 milhões de perdas económicas. O 2 atribuído às lesões e às doenças não fatais traduz-se em 2/50 fatalidades ou 2 milhões em perdas económicas ou em gastos em medidas de mitigação.

O nível cumulativo de custos, perdas económicas, fatalidades e outros impactos ao longo da duração dos cenários CIP/DSS é que determinam a preferência relativa das opções de mitigação.

Posteriormente, o CIP/DSS-DM cria gráficos que revelam quais as melhores estratégias de mitigação alternativas produzem resultados mais favoráveis, sob diferentes condições de ameaça. A ferramenta constrói ainda curvas de satisfação/arrependimento que divulgam a probabilidade de um decisor estar satisfeito com uma determinada estratégia de mitigação, caso ocorra um incidente. A Figura 6 representa as curvas de satisfação/arrependimento e a Figura 7 representa o quadro com a informação que pode ser extraída das curvas da análise de comparação entre opções de mitigação, em caso de uma infeção de varíola (Samsa *et al.*, 2008).

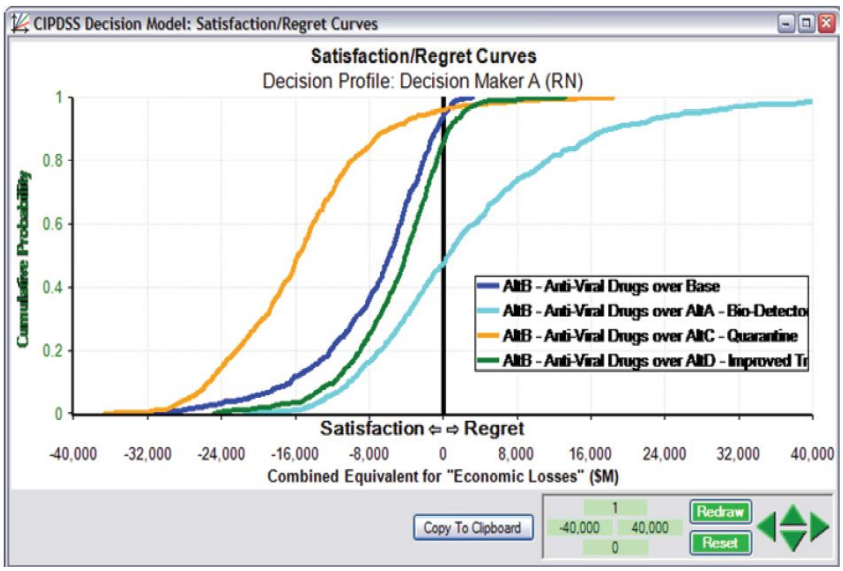
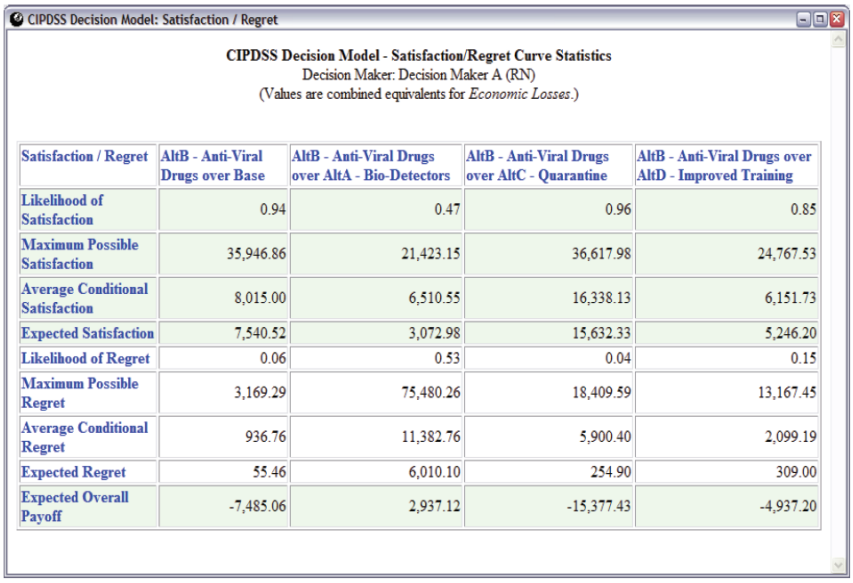


Figura 6 - Curvas Satisfação/Arrependimento (Samsa *et al.*, 2008)



CIPDSS Decision Model: Satisfaction / Regret

CIPDSS Decision Model - Satisfaction/Regret Curve Statistics
Decision Maker: Decision Maker A (RN)
(Values are combined equivalents for *Economic Losses*.)

Satisfaction / Regret	AltB - Anti-Viral Drugs over Base	AltB - Anti-Viral Drugs over AltA - Bio-Detectors	AltB - Anti-Viral Drugs over AltC - Quarantine	AltB - Anti-Viral Drugs over AltD - Improved Training
Likelihood of Satisfaction	0.94	0.47	0.96	0.85
Maximum Possible Satisfaction	35,946.86	21,423.15	36,617.98	24,767.53
Average Conditional Satisfaction	8,015.00	6,510.55	16,338.13	6,151.73
Expected Satisfaction	7,540.52	3,072.98	15,632.33	5,246.20
Likelihood of Regret	0.06	0.53	0.04	0.15
Maximum Possible Regret	3,169.29	75,480.26	18,409.59	13,167.45
Average Conditional Regret	936.76	11,382.76	5,900.40	2,099.19
Expected Regret	55.46	6,010.10	254.90	309.00
Expected Overall Payoff	-7,485.06	2,937.12	-15,377.43	-4,937.20

Figura 7 – Quadro informativo relativo às curvas Satisfação/Arrependimento

2.4.6 Análise e Modelação da Proteção de Infraestruturas Críticas (CIPMA)

O projeto CIMPA foi uma iniciativa do Governo Australiano que resultou no desenvolvimento de uma ferramenta de *software* que combina modelos de simulação, bases de dados, sistemas de informação geográfica (SIG) e modelos económicos. O SIG é o núcleo deste sistema pois é utilizado para reunir dados, modelar e visualizar resultados.

A ferramenta desenvolvida pelo projeto CIMPA é aplicada nos sectores bancário e financeiro, da energia e das telecomunicações, tendo em consideração todos os perigos,

naturais e humanos. Destina-se a legisladores e indústrias para a avaliação de diferentes cenários de interrupção de infraestruturas críticas e a decisores a nível nacional.

A metodologia utilizada na ferramenta foca-se em quatro áreas principais:

- Consequências da falha de uma infraestrutura crítica: visualização em GIS das consequências económicas e populacionais, duração da falha, dinâmica de sistemas de infraestruturas críticas;
- Falha de pontos singulares: identificação de pontos particularmente vulneráveis que podem desencadear efeitos cascata importantes;
- Riscos: Elaboração de mapas de riscos;
- Estratégias de mitigação e investimento.

Supondo que são aplicadas medidas que têm como objetivo minimizar o impacto das ameaças, e não diminuir a probabilidade, pode considerar-se que a resiliência está implícita nesta metodologia. Aliás, de acordo com os autores desta ferramenta, o seu objetivo é assistir na recuperação, concluindo-se assim que a resiliência é parcialmente abordada (Giannopoulos *et at.* 2012).

2.4.7 *CommAspen*

A *CommAspen* é a evolução da primeira versão de uma ferramenta de modelação *agent-based* que permite modelar as interdependências entre sistemas de energia elétrica e outras infraestruturas (Barton, 2004). Um modelo *agent-based* é um, de uma classe de modelos computacionais que permite simular as ações e iterações de agentes autónomos, tanto entidades individuais como coletivas, de forma a avaliar os seus efeitos no sistema como um todo (Grimm, 2005).

A ferramenta de avaliação de impacto, *CommAspen*, criada pelos Estados Unidos, foca-se principalmente nos sectores da energia elétrica, telecomunicações e finanças. Assim que existe uma decisão ou evento no sector das telecomunicações, a ferramenta modela o comportamento do sistema de infraestruturas interdependente. Nesta fase, as dependências do sector das telecomunicações com outas infraestruturas, não são consideradas.

As técnicas de modelação *agente-based* e a configuração do arquivo de entrada, que permite executar a análise, são características que requerem um certo nível de especialização, sendo a ferramenta *CommAspen* extremamente técnica.

O sistema de rede que suporta infraestruturas para transações financeiras é modelado através de um agente dedicado, isto permite que seja modelado o impacto da interrupção da rede em infraestruturas dependentes.

As infraestruturas de comunicação, nesta abordagem, não são consideradas como sectores/infraestruturas separados, mas sim como uma camada subjacente integrada com a infraestrutura que é analisada (Barton, 2004). A resiliência não é abordada nesta metodologia.

2.4.8 DECRIS *Approach*

A abordagem DECRIS constrói-se através das metodologias sectoriais de avaliação de riscos já existentes na Noruega, com a intenção de propor uma metodologia genérica e intersectorial de avaliação de riscos e vulnerabilidades que aborde todos os perigos.

A DECRIS baseia-se num procedimento com os seguintes passos (Utne *et al.*, 2012):

1. Identificação de taxonomias do evento e dimensões de risco;
   - **a)** Estabelecer uma taxonomia/hierarquia dos eventos indesejados. A taxonomia DECRIS tem as seguintes categorias de eventos principais: eventos naturais, eventos técnicos/humanos (erros/acidentes) e atos maliciosos.
   - **b)** Decidir as dimensões das consequências utilizadas para analisar os eventos indesejados. A DECRIS define as seguintes categorias de consequências: vida e saúde, ambiente, economia, capacidade de gestão, confiança política e disponibilidade de entrega/fornecimento de infraestrutura.
   - **c)** Calibrar matrizes de risco. Os eventos indesejados são descritos com uma categoria de probabilidade e uma categoria de consequências para cada categoria de probabilidade. Estas categorias devem ser estabelecidas e a sua discussão é necessária, de forma calibrar as matrizes de risco resultantes.
2. Análise simplificada de riscos e vulnerabilidades para os eventos identificados;
   - **a)** Identificar todos os eventos (perigos) indesejados.
   - **b)** Avaliar os riscos associados a cada evento indesejado. Na análise simples, são consideradas as duas dimensões vida e saúde edisponibilidade de entrega/fornecimento da infraestrutura.

3. Seleção dos eventos a serem analisados detalhadamente. Potenciais candidatos geralmente têm risco elevado. Na DECRIS são fornecidas informações específicas para apoiar a seleção, como um evento ter potencial de acidente grave, de haver dependências relevantes, em funções críticas de segurança, e na existência de desafios de comunicação relacionados com o evento;
4. Análise detalhada dos eventos selecionados. O curso dos eventos e várias consequências são investigados com mais detalhe. Estas análises devem incluir:
   a) Avaliação de interações e outras ligações entre infraestruturas e como isso afeta as consequências dos eventos indesejados;
   b) Avaliação de vulnerabilidades (junções críticas ou barreiras fracas);
   c) Sugerir e avaliar medidas de redução de risco e vulnerabilidade.

O processo de seleção de riscos a serem analisados detalhadamente apoia-se na importância do risco, na quantidade de infraestruturas afetadas e na dificuldade de comunicação dos eventos ao público. A questão de comparabilidade das consequências de um evento em diferentes infraestruturas permanece aberta (Giannopoulos *et al.*, 2012) Governos locais, municípios e empresas responsáveis por infraestruturas críticas são o grupo alvo desta metodologia que foi aplicada em Oslo, Noruega, nos sectores de fornecimento de energia elétrica, abastecimento de água, transportes e sistemas de informação e comunicação (Utne *et al.*, 2012).

De forma a alargar a compreensão das interdependências entre sectores, a metodologia DECRIS promove a colaboração entre *stakeholders* dos diferentes sectores. Esta metodologia não tem em consideração a resiliência (Giannopoulos *et al.*, 2012)

2.4.9 Metodologias Europeias de Avaliação de Risco e de Planeamento de Contingências para Redes de Energia Interligadas (EURACOM)

EURACOM é um projeto que pretende desenvolver uma abordagem comum e holística para gestão de risco e métodos de planeamento de contingência.

O objetivo é criar infraestruturas do sector da energia mais resilientes, desenvolvendo metodologias e ferramentas que assegurem o diálogo, a partilha de informação e cooperação entre operadores do sector da energia, utilizadores de energia, fornecedores de soluções de segurança, administradores, entidades reguladoras e outros *stakeholders*.

Esta metodologia requer a utilização da mesma metodologia em toda a rede, desde a produção à distribuição, e em todos os diferentes níveis hierárquicos, desde empresas individuais ao nível europeu. EURACOM deve ser aplicável a todos os perigos a que o sector está sujeito (SFP, 2011).

EURACOM não se considera uma metodologia, mas sim uma estrutura de uma metodologia, visto que ainda não foram desenvolvidas ferramentas de suporte e implementação da metodologia. A metodologia dirige-se a decisores e legisladores e consiste nos seguintes passos (Giannopoulos *et al.*, 2012), ilustrados na Figura 8:

1. Organizar uma equipa holística com visões holísticas;
2. Definir o âmbito holístico;
3. Definir escalas de avaliação de risco;
4. Compreender os ativos;
5. Compreender o contexto da ameaça;
6. Verificar a segurança/Identificar as vulnerabilidades;
7. Avaliar e classificar os riscos.

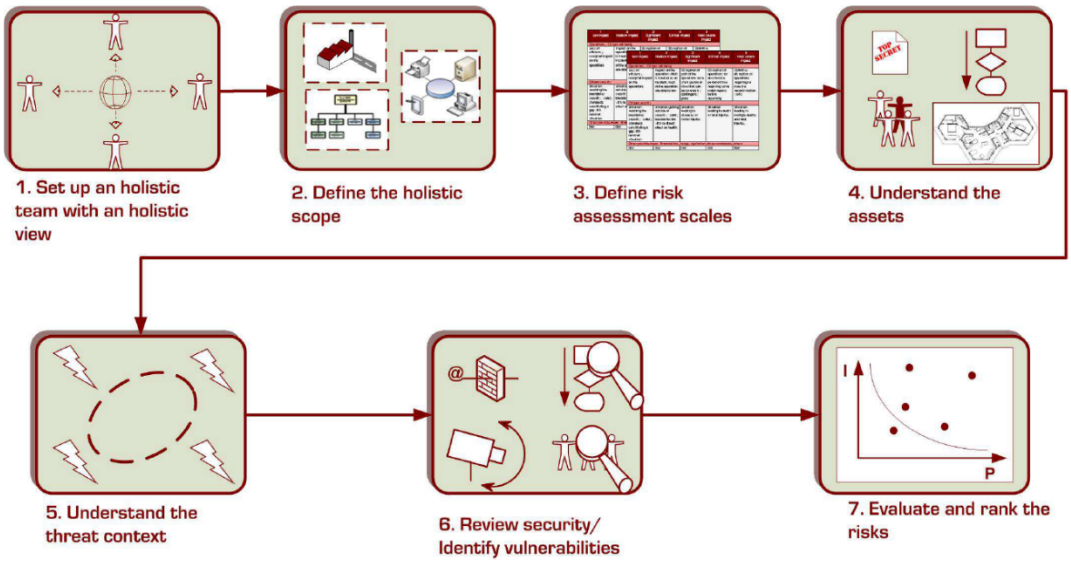


Figura 8 - Abordagem de avaliação de risco (SFP, 2011)

Uma abordagem holística ou gestão holística de riscos visa gerir os riscos utilizando uma abordagem conjunta que exige a consideração das seguintes dimensões: segurança física, segurança das tecnologias de informação e comunicação, segurança organizacional e aspetos de fator humano relativos à segurança. Estas dimensões serão utilizadas para

analisar cada um dos seguintes componentes do risco: ativos, vulnerabilidades, ameaças e efeitos.

A definição do âmbito, ponto 2, deve ter a sua realidade definida de um ponto de vista holístico, ou seja, deve ter um perímetro físico incluindo ativos físicos, deve ser composto por sistemas e redes definidas, deve ter limites de um ponto de vista organizacional, com definição das várias funções de trabalho envolvidas.

As dependências da organização em relação a elementos fora do âmbito podem ser analisadas através dos resultados do projeto EURAM sobre a metodologia para análise de (inter)dependências.

A avaliação do risco, R é alcançada pela avaliação direta da probabilidade de ocorrência, P e a severidade, S, com R = P x S. Assim, é importante definir, no início do projeto, a escala contra a qual a probabilidade e a severidade serão avaliadas. Esta, por razões práticas, aconselha-se a ser uma escala qualitativa com valores de 1 a 5.

A componente probabilidade, avaliação da viabilidade de um ataque ou probabilidade de um acidente, toma os valores de probabilidade 1 muito baixa, 2 baixa, 3 média, 4 alta e 5 perto da certeza. Ao avaliar a probabilidade, as escalas devem ser ajustadas de acordo com dois tipos diferentes de eventos adversos: Ataques e acidentes não direcionados e direcionados. Para os ataques e acidentes não direcionados a avaliação da probabilidade é baseada em provas históricas, utilizando, por exemplo, experiência ou análise estatística; no caso dos ataques e acidentes direcionados, uma análise estatística não é apropriada pois apesar dos eventos ainda não terem acontecido, não significa que esses eventos não são viáveis ou que nunca irão acontecer. Assim, a melhor abordagem para a análise destes ataques e acidentes é avaliar a viabilidade do ataque, tendo em consideração fatores como atratividade do alvo, motivação/habilidades/recursos do atacante e nível de proteção do alvo.

A segunda componente que permite calcular o risco é a severidade, que permite a avaliação do impacto no fornecimento de produto/serviço, segurança dos cidadãos, imagem, confiança dos cidadãos, impacto financeiro ou outros aspetos, toma os valores de severidade 1 baixo impacto, 2 impacto médio, 3 impacto significativo, 4 impacto crítico e 5, impacto mais severo. Mesmo que os níveis de impacto e probabilidade tenham que ser adaptados no âmbito da análise, é necessário ter uma definição comum desses níveis, de forma a permitir a análise de interdependências entre infraestruturas críticas (SFP, 2011). A resiliência não é abordada nesta metodologia (Giannopoulos *et al.*, 2012).

2.4.10 Análise Rápida

Fast Analysis fornece ao DHS respostas em relação a ameaças a infraestruturas críticas. Estas análises são muitas vezes conduzidas em resposta a ameaças específicas e, por isso, devem ser realizadas rapidamente. Tendo isto em conta, desenvolveu-se a ferramenta *Fast Analysis Tool* (FAIT) que auxilia as análises rápidas (Kelic *et al.,* 2008).

FAIT desenvolvida no âmbito do programa *National Infrastructure Simulation and Analysis Center (NISAC)*, gerido pelo DHS, em colaboração com o Laboratório Nacional Sandia e o Laboratório Nacional Los Alamos, consiste numa síntese entre os dados de uma infraestrutura e o conhecimento especializado, que determina o significado e as interdependências de infraestruturas críticas americanas. Esta ferramenta destina-se a decisores e legisladores (Giannopoulos *et al.,* 2012).

FAIT representa uma ferramenta de avaliação do impacto e traduz-se em quatro elementos principais:

- Avaliação de interdependências;
- Co localização de infraestruturas críticas;
- Associação de informação;
- Impacto económico.

A primeira prioridade da ferramenta FAIT é a consideração das interdependências, que são tratadas com base em conhecimento especializado, codificado numa linguagem baseada em regras, de *software*s de sistemas de especialistas. Esta linguagem utiliza-se para expressar relações entre várias infraestruturas.

Todas as interdependências são consideradas nesta metodologia, no entanto as interdependências geográficas são tratadas de forma distinta, pois fazem parte do segundo elemento principal da metodologia, que retira as dependências geográficas dos ativos baseando-se em informação geoespacial relevante (Giannopoulos *et al.,* 2012).

O impacto económico é um elemento importante no que toca a avaliação e gestão de riscos. A metodologia FAIT determinava esse impacto económico através de modelos de entrada/saída, utilizando dados sobre a duração da interrupção e recuperação dos ativos (Giannopoulos *et al.,* 2012). No entanto, após a temporada de furacões no Atlântico, o NISAC desenvolveu a ferramenta de Contabilidade Económica Regional (*REAcct*) que recebeu um arquivo de entrada geoespacial, baseado nos modelos de entrada/saída

utilizados anteriormente. Esta ferramenta calcula rapidamente os efeitos diretos e indiretos associados com o evento, diminuindo o tempo de resposta (Stamber *et al.,* 2013).
A ferramenta FAIT aplica-se, maioritariamente a ativos de todos os setores, infraestruturas e suas interdependências e aborda todos os perigos. A resiliência não é considerada (Giannopoulos *et al.,* 2012).
A *FASTmap* é uma aplicação de mapeamento que complementa a ferramenta FAIT, desenvolvida pelo NISAC, que pesquisa dados de infraestruturas nacionais e recursos de emergência, sendo ainda possível configurar esta aplicação para exibir resultados de modelos independentes, gerando *output* geoespacial e/ou temporal. A aplicação gera mapas e relatórios de ativos em risco, em qualquer área de interrupção ou qualquer área de análise.
Em caso de ocorrência dos seguintes eventos: furacões, inundações, terramotos, incêndios florestais; a aplicação *FASTmap* responde a perguntas como: que ativos estão localizadas numa determinada área? Quantos ativos de um tipo específico se encontram na área? Qual a capacidade total dos ativos? Onde está localizado um ativo específico e quais são os seus atributos? (NISAC, 2017)

2.4.11 Multicamadas de Redes de Infraestruturas (MIN)

A metodologia MIN tem como objetivo generalizar o paradigma das redes de transportes para outras infraestruturas e instituir otimização.
A metodologia de avaliação de impacto baseia-se na teoria dos jogos, estudo de modelos matemáticos de conflito e cooperação entre decisores racionais e inteligentes, e na otimização sob múltiplas restrições e conceitos de confiabilidade da rede.
A análise executa-se com base em modelos e simulações *agent-based* permitindo determinar o fluxo de quantidades em estado estável e obter uma ótima alocação de recursos. As interdependências são abordadas capturando o fluxo dinâmico como input-output (modelo de Leontief) entre setores.
A metodologia MIN, desenvolvida na Universidade de Purdue nos Estados Unidos, requer um alto nível de especialização e conhecimentos técnicos limitando as áreas para a sua possível aplicação. A resiliência não é abordada (Giannopoulos *et al.,* 2012).

2.4.12 *Agent-Based Laboratory for Economics* (N-ABLE)

N-ABLE desenvolveu a ferramenta *N-ABLE* que consiste numa ferramenta de micro simulação *agent-based* que modela interdependências complexas entre sectores económico e de infraestruturas (Eidson *et al.,* 2005). A base teórica da metodologia é a teoria de redes complexas, (Albert *et al.,* 2002) e modelação *agent-based* para simulação. Os agentes N-ABLE são peças relativamente pequenas de código de computador que modelam agentes económicos como: empresas que utilizam *inputs* materiais, mão de obra, capital, energia elétrica, telecomunicações, transporte e serviços bancários para produzir e vender produtos; empresas de energia elétrica que produzem e vendem energia; consumidores e vendedores de energia elétrica; empresas de fabrico que gerem cadeias de produção e de distribuição; entre outros (Eidson *et al.,* 2005).

A identificação de quais os sectores económicos mais vulneráveis à interrupção das infraestruturas é o âmbito da metodologia de avaliação de impacto, N-ABLE. Esta ferramenta matematicamente sofisticada requer utilizadores especializados para obter resultados fidedignos.

N-ABLE dirige-se principalmente a investigadores e cientistas da área, no entanto podem beneficiar da mesma, operadores de infraestruturas críticas e legisladores, dependendo do seu nível de especialização. A resiliência não é abordada.

Uma vantagem importante desta metodologia está na possibilidade de aplicar a mesma a avaliação do impacto em redes de abastecimento, devido a interrupções (Giannopolous *et al.,* 2012).

2.4.13 Modelo de Operações baseado em Efeitos centrados na Rede (NEMO)

NEMO foi criado para ser utilizado em operações militares, como ferramenta de avaliação de operações em tempo real. Na ferramenta NEMO as infraestruturas dos oponentes são analisadas como um sistema de redes interligadas, contemplando assim todos os sectores. A sua base teórica baseia-se em ferramentas similares às utilizadas no apoio a estratégias militares, por exemplo para a avaliação de vulnerabilidades entre domínios (Goodwin *et al.,* 2005).

A identificação das interdependências nesta metodologia não tem a intenção de reduzir o impacto de um evento, mas sim identificar os elementos críticos da rede que podem maximizar o impacto através de efeitos em cascata (Giannopoulos *et al.,* 2012).

A ferramenta admite liberdade na definição das dependências, assim como possibilita relações *on/off*, ou seja, quando uma componente falha, as componentes que dependem desta, desligam automaticamente. Outra relação possível consiste nas componentes desligarem, um determinado período de tempo após a componente da qual dependem falhar (Goodwin *et al.,* 2005). São postuladas formas ideais, por exemplo *net-centric*, que se refere "*a participar como parte de uma comunidade complexa e em constante evolução de pessoas, dispositivos, informações e serviços interligados por uma rede de comunicações para obter o melhor benefício dos recursos e uma melhor sincronização de eventos e das suas consequências*" (Sirohi, 2016).

A análise realizada através da metodologia NEMO oferece uma gestão de consequências com relação ao efeito mais próximo e, ainda, com efeitos de segunda ordem distribuídos por toda a infraestrutura. Estes resultados são mapeados em SIG (Giannopoulos *et al.,* 2012).

As duas capacidades críticas do NEMO são: gestão de consequências, que identifica e quantifica os efeitos não intencionais de uma operação, e análise do curso de ação, aplica-se ao planeamento de campanhas e à segurança interna, sendo utilizada para proporcionar uma maneira de conduzir análises de vulnerabilidades das infraestruturas e apoiar a identificação de nós críticos que representam um maior impacto, em caso de ataques terroristas (Goodwin *et al.,* 2005).

Enquanto a gestão de consequências verifica o que poderia acontecer, se algo suceder de uma certa forma, a análise do curso de ação examina as várias formas de realizar uma tarefa, de forma a determinar qual delas atinge o objetivo pretendido.

Autoridades militares são o grupo principal a que esta metodologia se destina, no entanto, operadores de infraestruturas críticas e decisores podem beneficiar com a utilização desta ferramenta, pois esta permite identificar pontos vulneráveis de ativos e infraestruturas. Deve-se ter em conta que a ferramenta necessita de pessoal especializado (Goodwin *et al.,* 2005).

A resiliência encontra-se implícita no âmbito da metodologia através das medidas de proteção e recuperação (Giannopoulos *et al.,* 2012).

2.4.14 Modelação da Avaliação de Risco da Segurança de Redes (NSRAM)

NSRAM desenvolvida pela Universidade James Madison, engloba todas as infraestruturas interligadas e pretende determinar a interação e resposta dos sistemas a todos os tipos de acidentes e ataques.

Esta metodologia é fundamentada em simulações de modelos *agent-based*, em ambiente estocástico, incluí eventos de falha, como a maioria das metodologias descritas, no entanto integra também a capacidade de reparação, que permite modelar os efeitos do pessoal de reparação ou escassez de peças, requisitos de comunicação e incerteza. Esta capacidade permite modelar o comportamento humano no caso de falhas do sistema (Baker *et al.*, 2003).

A análise dos modelos faculta o desempenho do serviço do sistema com medidas de segurança e risco ao longo do tempo, identifica ainda os modos de falha mais graves, implementando contramedidas rentáveis e planeando a reconstituição. A resiliência é considerada neste ponto, principalmente no processo de recuperação.

A NSRAM confere enfâse à interatividade e interligação entre as infraestruturas simultaneamente. Esta destina-se a operadores de infraestruturas críticas e decisores (Giannopoulos, 2012).

2.4.15 RAMCAP-*Plus*

RAMCAP-*Plus*, desenvolvida pela Sociedade Americana de Engenheiros Mecânicos, corresponde a uma metodologia que permite identificar, priorizar e coordenar a preparação de infraestruturas críticas, incluindo proteção, prevenção de eventos perigosos ou suas consequências, e a resiliência, retorno rápido para a função completa após a ocorrência desses eventos. Esta metodologia aborda todos os perigos, é adaptável a vários sectores e dirige-se a oficiais de segurança governamentais e de indústrias (Brashear *et al.*, 2009).

O processo RAMCAP – *Plus* compreende sete passos (Brashear *et al.*, 2009). Tomados como um todo, estes passos fornecem uma base rigorosa, objetiva, replicável e transparente para coleta de informação, interpretação, análise e decisão.

1. Caracterização dos ativos

Neste ponto, analisa-se a missão da organização e os requisitos operacionais, de forma a determinar quais os ativos que podem diminuir a capacidade de uma instalação cumprir

a sua missão; para os ativos críticos identificados faz-se uma estimativa preliminar das potenciais consequências, de várias ameaças ou perigos, em termos ordinais.

Os ativos avaliados (p.e. rede de água e esgotos), incluem outros ativos que estão diretamente envolvidos na realização das missões ou funções mais importantes (p.e. condutas, estações elevatórias, etc.), que os suportam (p.e. eletricidade, químicos, monitorização automática, etc.) e outras infraestruturas das quais dependem (p.e. estações de eletricidade). Estes ativos podem incluir instalações físicas, sistemas informáticos, bases de conhecimento, recursos humanos, clientes ou fornecedores críticos fora do local.

2. Caracterização das ameaças

A caracterização de ameaças consiste na identificação e descrição de cenários de ameaças de referência, em detalhe suficiente que permita estimar a vulnerabilidade e as consequências. Na Tabela 4 encontra-se uma ampla variedade de cenários de ameaças.

Tabela 4 - Resumo de cenários de ameaças de referência (Brashear *et al.*, 2009)

Attack Type	Tactic/Attack Description			
Marine	**M1** Small boat	**M2** Fast Boat	**M3** Barge	**M4** Deep draft shipping
Aircraft	**A1** Helicopter	**A2** Small Plane (Cessna)	**A3** Medium, Regional Jet	**A4** Large Plane Long-Flight Jet
Land-based Vehicle	**V1** Car	**V2** Van	**V3** Mid-size Truck	**V4** Large Truck (18 wheeler)
Assault Team	**AT1** 1 Assailant	**AT2** 2-4 Assailants	**AT3** 5-8 Assailants	**AT4** 9-16 Assailants
Sabotage	**S(PI)** Physical-Insider	**S(PU)** Physical-Outsider	**S(CI)** Cyber-Insider	**S(CU)** Cyber- Outsider
Theft or Diversion	**T(PI)** Physical-Insider	**T(PU)** Physical- Outsider	**T(CI)** Cyber-Insider	**T(CU)** Cyber- Outsider
Product Contamination	**C(C)** Chemical	**C®** Radionuclide	**C(B)** Biotoxin	**C(P)** Pathogenic
	C(W) – Weaponization of waste disposal system			
Natural Hazards	**N(H)** Hurricanes	**N(E)** Earthquakes	**N(T)** Tornadoes	**N(F)** Floods
Dependency & Proximity Hazards	**D(U)** Loss of Utilities	**D(S)** Loss of Suppliers	**D(S)** Loss of Employees	**DI** Loss of Customers
	D(T) Loss of Transportation		**D(P)** Proximity to other targets	

A utilização de um conjunto comum de ameaças de referência é um ponto chave para a comparabilidade dos resultados. Cinco tipos distintos de ameaças de referência são definidos na RAMCAP – *Plus*:

- Terrorismo, ataques de inimigos tendo em conta os meios, métodos, motivações e capacidades dos terroristas;

- Perigos naturais, atualmente inclui furacões, inundações, tornados e terramotos, com base na localização física da instalação e informação federal;
- Contaminação do produto ou dos fluxos de resíduos, sugerida pelo sector da água, sendo também aplicável aos alimentos e produtos farmacêuticos. Aborda as preocupações de contaminação acidental e intencional;
- Perigos das cadeias de abastecimento, dependências imediatas, principalmente questões da cadeia de abastecimento, como fornecedores, mão-de-obra, clientes, etc. Incluídas como um passo inicial para lidar com dependências de outras organizações para elementos críticos da missão da organização;
- Perigos de proximidade, potencial para se tornarem danos colaterais de eventos em locais próximos.

A organização decide quais dos cenários definidos representam ameaças fisicamente possíveis para a instalação. Para estas ameaças avaliam-se sumariamente as consequências de um ataque bem-sucedido por cada ameaça, para cada ativo identificado como crítico. Uma maneira de fazer essa avaliação é através de uma matriz dos ativos críticos *versus* as possíveis ameaças e estimar de acordo com uma escala ordinal de cinco a sete pontos (p.e. muito baixo, baixo, moderado, alto e muito alto).

3. Análise das consequências

Identifica e estima as piores consequências razoáveis geradas por cada combinação específica de ativo/ameaça. Este ponto examina o projeto, *layout* e a operação da instalação de forma a estimar fatalidades, lesões graves e impactos económicos. Os impactos económicos são definidos na RAMCAP-*Plus* em dois níveis: as consequências económicas para a organização e consequências económicas para a comunidade metropolitana regional que a organização serve.

4. Análise das vulnerabilidades

A análise de vulnerabilidades estima a probabilidade condicional de que as consequências estimadas ocorram aquando da ocorrência de uma ameaça ou perigo específicos. A análise de vulnerabilidades envolve uma verificação das capacidades de segurança existentes, componentes estruturais e contramedidas existentes e a sua eficácia. Existem várias ferramentas que permitem analisar vulnerabilidades, Tabela 5.

Tabela 5 - Ferramentas para análise de vulnerabilidades (Brashear *et al.*, 2009)

Method	Description
Direct Expert Elicitation	Members of the evaluation team discuss the likelihood of success and their reasoning for their estimates; in its more formal form, a statistical "Delphi" processor Analytical Hierarchy Process can be used to establish a consensus
Vulnerability Logic Diagrams (VLDs)	Plot of the flow of events from the time an adversary approaches the facility to the terminal event in which the attack is foiled or succeeds, considering obstacles and countermeasures that must be surmounted, with each terminal event associated with a specific likelihood estimate. This is frequently complemented with an estimate of the reaction time of a counterforce once the attack has been detected
Event Trees (also called "failure trees")	Tree with branches the sequence of events between the initiation of the attack and the terminal events The evaluation team estimates the probability of each outcome. Multiplying the probabilities along each branch, from the initiating event to each terminal event, calculates the probability of each unique branch, while all branches together sum to 1.0. The sum of the probabilities of all branches on which the attack succeeds is the vulnerability estimate.
Decision Trees	Very similar to event trees except that the decisions by the adversary are modeled at each node in the unfolding tree to capture the adaptive behavior of the adversary; a sophisticated variant is conceive the tree as a two-player game
Hybrids of These	Often used by the more sophisticated assessment teams

5. Avaliação das ameaças

Estima a probabilidade de uma ameaça em particular ocorra num determinado período de tempo, geralmente um ano. A abordagem difere consoante o tipo de perigo, Tabela 6.

Tabela 6 - Estimativa da probabilidade de um perigo (Brashear *et al.*, 2009)

Hazard Type	Likelihood/Probability Estimation
Terrorist attack	Based on the terrorists' objectives and capabilities, generally (provided by intelligence and law enforcement agencies), and the attractiveness of the facility relative to alternative targets, the asset's expected value (vulnerability x consequences), and the cost/effectiveness of the attack.
Natural hazards	Based on the historical Federal frequency data for various levels of severity at the specific location of the asset. Can be adjusted if there is reason to believe that the future frequency or severity will differ from the past.
Dependency hazard	Based on local historical records for the frequency, severity and duration of service denials as a baseline estimate of "business as usual," incrementally increased if they may be higher due to terrorist activity or natural events on required supply chain elements. Confidential conversations with local utilities and major suppliers can inform these estimates.
Product contamination	Treated the same as terrorism and dependency likelihood, except additional consideration is given to accidental contamination of inputs and the vulnerability of critical processes to accidents.
Proximity hazard	Based on asset's location relative to other assets that may incur adverse events leading to collateral damage, using the same logic in estimating terrorist and natural hazard threats.

A probabilidade de terrorismo, e a sua contribuição para a contaminação, proximidade e até mesmo riscos de dependência, é a mais difícil de estimar, estando ainda a ser refinada (Brashear *et al.*, 2009).

6. Avaliação do risco e da resiliência

Cria a base para a priorização e seleção entre redução de risco e resiliência. O passo de avaliação de risco é uma avaliação sistemática e abrangente das estimativas previamente desenvolvidas. O risco para cada ameaça, para cada ativo, é calculado a partir da relação de risco expressa na equação (2.3), em que T – Ameaça, V – Vulnerabilidade e C - Consequência.

$$Risco = T\ x\ V\ x\ C \tag{2.3}$$

A resiliência, capacidade de funcionar apesar e durante um evento traumático ou restaurar a funcionalidade em período de tempo curto, é determinada através da equação (2.4), no caso do proprietário, e através da equação (2.6), no caso da comunidade, para cada par ativo/ameaça.

$$Resiliência_{Proprietário} = LNR\ x\ V\ x\ T \tag{2.4}$$

LNR – *Lost net revenue* (receita líquida perdida), equação (2.6).

$$LNR = \ DD\ x\ SD\ x\ (UP - VC) \tag{2.5}$$

A receita líquida perdida corresponde ao produto da negação do serviço, DD em dias, e a severidade da negação do serviço, SD em unidades físicas por dia, e o preço do serviço antes do evento, UP menos custos variáveis evitados, VC, em dólares por unidade, todos os quais são partes essenciais para calcular o prejuízo financeiro do proprietário.

$$Resiliência_{Comunidade} = LCEA\ x\ V\ x\ T \tag{2.6}$$

LCEA – *Lost Community Economic Activity* (Atividade económica da comunidade perdida)

A atividade económica da comunidade perdida corresponde à quantidade de diminuições nas perdas de rendimento, tanto diretas como indiretas, em toda a economia da região metropolitana devido à negação do serviço. Geralmente é estimado como uma função da receita perdida do ativo e da duração da negação do serviço, usando uma aplicação estática de dados econômicos regionais básicos e um modelo de *input-output*, modificado para refletir a resiliência dos respetivos setores de negócios. Os impactos sobre o número

de postos de trabalho e nível de emprego também são frequentemente estimados no mesmo modelo (Rose, 2006 e MMC, 2005).

7. Gestão do risco e da resiliência

O ponto gestão de risco e resiliência corresponde ao passo em que se reduz o risco e aumenta-se a resiliência. Tendo determinado o risco e a resiliência de cada par importante ativo/ameaça, este passo define novas medidas de segurança e opções de resiliência, de mitigação e de consequências, sendo depois avaliadas de forma a alcançar um portfólio que gere um nível aceitável de risco e resiliência, a um custo aceitável. Na Tabela 7 encontram-se as ações que constituem este sétimo e último passo (Brashear *et al.*, 2009).

Tabela 7 - Ações de gestão de risco e resiliência (Brashear *et al.*, 2009)

Act. No.	Activity
1. Acceptance Level	Establish whether the risk/resilience level is acceptable.
2. Design	Design potential countermeasures and consequence-mitigation options that would reduce risk and/or enhance resilience.
3. Costs	Estimate the investment and operating costs of each option.
4. Re-estimation	Re-estimate consequences, threat likelihood and/or vulnerability, whichever is affected by the option.
5. Benefits	Re-calculate risk and resilience, given the option, and subtract it from the risk without the option (the "do nothing" baseline option) to define the *benefit* of the option.
6. Combinations	Combine the options that affect multiple asset/threat pairs, e.g., if a higher fence changes the vulnerability for an attack by one assailant, it may do the same for two to four. Add the benefits of the asset/pairs to be the total benefit of the option.
7. Key Metrics	Calculate the net benefits (less costs) – value – and the benefit/cost ratio – efficiency – of the option.
8. Rank & Select	Select the options that have the highest net benefits and/or benefit/cost ratios and the lives saved and injuries avoided, considering both risk and resilience until resources are fully committed (less any reserved amounts).
9. Manage	Manage the implementation and operation of the selected options, evaluate their effectiveness and make mid-course corrections for maximum effectiveness.
10. Recycle	Repeat the risk analysis cycle periodically or as needed given intelligence or changing circumstances, e.g., new technologies, new facilities.

A metodologia tem uma abordagem simples, intersectorial que apesar de ser baseada em técnicas de avaliação de riscos existentes, corresponde a uma abordagem de alto nível. Evita-se detalhe desnecessário pois a RAMCAP-*Plus* foca-se nos ativos mais críticos de uma instituição. Ao contrário das metodologias analisadas até este ponto, a metodologia RAMCAP-*Plus* tem a resiliência como um elemento central (Giannopoulos *et al.*, 2012).

2.4.16 Análise de Risco e Vulnerabilidade (RVA)

RVA metodologia desenvolvida pela Agência Dinamarquesa de Gestão de Emergência, pretende avaliar ameaças, riscos e vulnerabilidades das funções que são particularmente críticas para o funcionamento eficaz da sociedade.

Na Dinamarca, de acordo com o Ato de Preparação, legislação desse país, todas as entidades governamentais centrais são responsáveis pelo planeamento de preparação. De acordo com a secção 1, do Ato de Preparação Dinamarquês: "*No âmbito de suas respetivas áreas de atuação, ministros individuais devem planear a manutenção e a continuidade das funções da sociedade, em caso de acidentes e catástrofes, incluindo ações de guerra, e de forma a proporcionar apoio às forças de defesa*".

A análise dos riscos e vulnerabilidade pode gerar benefícios em várias áreas, dentro de contextos como criação de uma visão geral, priorização, decisão, coordenação, treino e comunicação (DEMA, 2006).

A metodologia RVA desenvolveu-se de forma a cumprir a legislação do país e aplica-se através de um modelo baseado principalmente em informação qualitativa, o que significa que a análise não será puramente objetiva. É necessário ter em conta que a análise será afetada por experiências passadas, competências e convicções dos participantes (DEMA, 2006).

O modelo RVA consiste em quatro *templates* em *MSWord*, sendo que a análise é feita preenchendo os campos e fazer escolhas usando os menus *dropdown*. Os passos do modelo são os seguintes (DEMA, 2006):

1. Ponto de partida para a análise – Identificação dos participantes, responsabilidade na preparação da organização e decisão em relação a quais serão funções críticas a abordar;
2. Identificação das ameaças – Formular um ou mais cenários realísticos que sejam representativos de diferentes tipos de ameaças, com o objetivo de restringir o campo de potenciais ameaças, de forma a concentrar análise em áreas que sugerem que podem existir riscos e vulnerabilidade substanciais;
3. Análise de cenários de ameaças – Análise de riscos e vulnerabilidades para cada um dos cenários indicados no ponto 2. Neste ponto utiliza-se índices para avaliar, numa primeira fase, a probabilidade de ocorrência e as consequências, resultando num nível de risco geral; e na segunda fase, avaliar as vulnerabilidades, tendo em conta a capacidade da organização de neutralizar, gerir e recuperar de determinado evento;
4. Perfil de risco e vulnerabilidade – Comparação dos resultados das várias análises realizadas no ponto 3. Resulta num perfil de risco e vulnerabilidades que fornece uma visão geral coletiva de quais tipos incidentes constituem o maior perigo.

Primeiro, cada cenário é colocado numa matriz de risco com base nas avaliações da probabilidade e das consequências, gerando uma clara apresentação gráfica dos níveis de risco, o que permite a comparação entre cenários.

Numa segunda fase, cada cenário é colocado numa visão de vulnerabilidades, resultando numa visão geral de vulnerabilidades que indica como a organização é resiliente ou vulnerável no que toca à neutralização, gestão e recuperação aos incidentes descritos no cenário.

Os *templates* do modelo RVA encontram-se disponíveis no site da DEMA (*Danish Emergency Management Agency)* onde é disponibilizado um guia de aplicação, com uma explicação passo por passo dos pontos acima descritos. Este guia contém nos Anexos A e B, respetivamente as funções críticas consideradas e um catálogo de ameaças. A metodologia RVA abrange todos os sectores de infraestruturas críticas e todos os perigos, naturais e humanos (DEMA, 2006).

A metodologia RVA destina-se principalmente a entidades governamentais, no entanto outras entidades com responsabilidade civil, tanto públicas como privadas podem beneficiar da sua utilização (Giannopoulos *et al.*, 2012).

2.4.17 Metodologia de Avaliação de Risco Sandia (SRAM)

A SRAM desenvolvida pelo Laboratório Nacional Sandia (SNL) nos Estados Unidos, apresenta os seguintes passos (Jaeger *et al.*, 2008):

1. (Etapa opcional) Triagem de alto nível na qual o utilizador pode identificar e priorizar várias instituições com base num conjunto definido de critérios de consequência;
2. Planeamento, fornece metas de avaliação e âmbito do projeto, identificação dos membros da equipa e ferramentas ou equipamentos necessários, missões da instalação definidas, preocupações de segurança da instalação e eventos indesejados;
3. Caracterização da instalação, inclui a coleta de informação de instalações, o desenvolvimento de uma árvore de falhas específica do local e a identificação de alvos potenciais;

4. Avaliação de consequências, o utilizador aplica ou adapta uma tabela de consequência padrão, ou desenvolve uma nova tabela de consequências, enumera os eventos indesejados e os alvos que, se atacados, podem causar um evento indesejado e fornece *input* para cada critério de consequência, para estimar o nível de gravidade dos eventos indesejados;
5. Avaliação de ameaças, permite ao utilizador identificar ameaças internas e externas e definir os seus motivos, objetivos e capacidades. Se existir informação suficiente pode ser estimada o potencial da ameaça, que considera a probabilidade de ataque;
6. Objetivos de proteção, inclui a identificação dos objetivos do local para o sistema de proteção. A eficácia do sistema de proteção é avaliada em que medida estes objetivos podem ser cumpridos;
7. Eficácia do sistema, o utilizador primeiro estima a estratégia mais provável do adversário para causar o evento indesejado e afetar os alvos associados. Um diagrama de caminho adversário é desenvolvido, que inclui uma representação gráfica da instituição que inclui camadas ou áreas e elementos de caminho entre essas camadas ou áreas. Usando um banco de dados de segurança física do SNL, derivado de muitos anos de testes e revisão de peritos, SME os atributos de salvaguarda para cada um dos elementos de caminho são definidos. Uma análise de caminho é então realizada para estimar o nível de eficácia do sistema de proteção para atender aos seus objetivos de proteção especificados. Finalmente, uma lista de possíveis vulnerabilidades ou vulnerabilidades de segurança é identificada para as funções de deteção, atraso e resposta do sistema de proteção física, PPS quando a eficiência do sistema é avaliada como baixa;
8. Valor do risco de segurança é estimado tendo em conta a probabilidade de um adversário causar um evento indesejado e a consequência que lhe está associada;
9. Determinar se o risco é aceitável;
10. Se o risco for demasiado elevado, o utilizador pode identificar possíveis medidas de redução de risco e avaliar o seu impacto. São desenvolvidos os pacotes de atualização e são fornecidas aos decisores as mudanças no risco, possíveis custos e impactos nas operações, cronograma e outras áreas;
11. Relatório dos resultados da avaliação e medidas para ajudar a apoiar os gerentes de risco a tomar decisões.

A SRAM é aplicada através de uma ferramenta *software*. Os passos descritos acima encontram-se ilustrados na Figura 9 que corresponde ao diagrama de fluxo de processo da metodologia de gestão de risco.

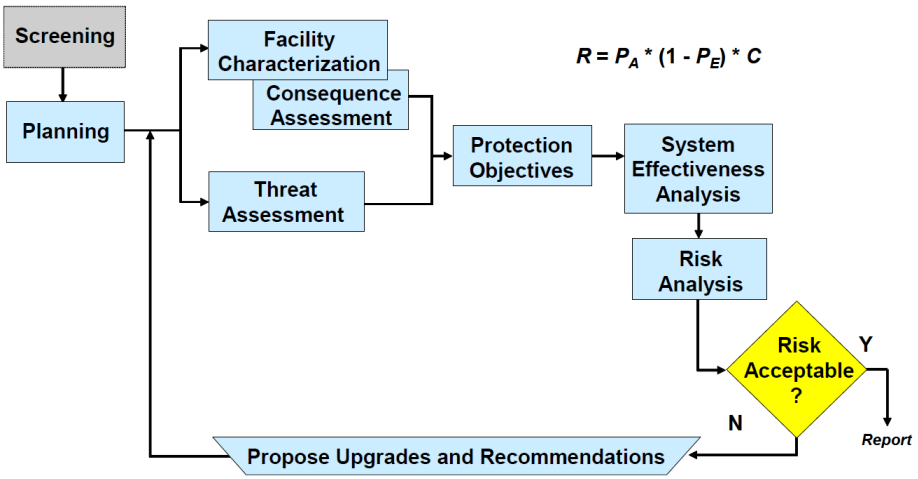


Figura 9 - Processo da metodologia da gestão de risco (Jaeger *et al.*, 2008)

Na avaliação de consequências é determinado um valor qualitativo de consequência (i.e. muito elevado, elevado, moderado, baixo e muito baixo) para todos os eventos indesejados identificados. Se não existirem valores para alguns dos eventos indesejados, podem ser determinados por especialistas da equipa. Assim que a matriz de consequência esteja estabelecida, é atribuído um valor de consequência apropriado a cada evento. De forma a avaliar as consequências, podem ser utilizadas as seguintes medidas de consequências: perda de vida, lesões graves, perda de missões/operações críticas, duração da perda, perda económica (instituição e comunidade), impacto psicológico, impacto para segurança nacional e outros, conforme especificado pela instituição (Jaeger *et al.*, 2008).

Na avaliação de risco, caso o utilizador opte por utilizar o risco condicional, para cada par ativo/ameaça, de forma a ser possível a comparação entre infraestruturas da mesma instituição, então o risco determinado através da ferramenta RAM usará uma metodologia de análise qualitativa e estima o risco condicional, equação (2.7) (Jaeger *et al.*, 2008):

$$Risco\ condicional = função\ (vulnerabilidade, consequência) \qquad (2.7)$$

Se o utilizar optar por estimar o potencial de ameaça a ferramenta RAM determina um risco relativo, equação (2.8) (Jaeger *et al.*, 2008).

$$Risco\ relativo = função\ (ameaça, vulnerabilidade, consequência) \quad (2.8)$$

No que respeita ao risco relativo, que tem em consideração a ameaça, o potencial de uma ameaça varia em diferentes regiões geográficas e diferentes setores de infraestruturas críticas e existe uma grande incerteza na estimativa da probabilidade de ocorrência da ameaça. Assim, ao contrário do risco condicional, o risco relativo não permite a comparação em infraestruturas abrangentes.

Na Figura 9 encontra-se a equação (2.9) que permite determinar o risco relativo (R) que considera a probabilidade do ataque (P_A), a vulnerabilidade $(1 - P_E)$ que está associada à probabilidade do sistema de segurança ser eficaz contra a ameaça (P_E) e as consequências (C).

$$R = P_A * (1 - P_E) * C \quad (2.9)$$

A ferramenta utilizada para a identificação das vulnerabilidades, nesta metodologia, designa-se por análise de árvore de falhas (FTA) (Giannopoulos *et al.,* 2012). A FTA consiste numa técnica analítica, em que se define um evento indesejado, de forma a analisar o sistema no contexto do seu ambiente e operação. Esta análise resulta em todas as combinações básicas que levarão à ocorrência do evento indesejado definido (Vesely *et al.,* 1981).

A FTA aplica-se principalmente a ativos, no entanto é possível adaptar essa técnica de análise, de forma a ser aplicável a redes complexas. A aplicação da FTA permite identificar cenários de falhas e elementos críticos para um ativo em funcionamento.

Os passos tomados na metodologia SRAM mostram-se um pouco diferentes do tradicional. No caso das ameaças, esta metodologia começa por identificar os eventos indesejados e as consequências relevantes, reduzindo o número de ameaças que podem causar esse evento indesejado. Numa segunda fase, as ameaças priorizadas são alvo de uma análise tipo, ou seja, utilizando as metodologias de avaliações tradicionais. Nesta fase considera-se também a eficácia do sistema de proteção, que é expressa em termos de reduzir a probabilidade de uma ameaça ter sucesso. Por fim, avalia-se se o risco é aceitável ou não. Caso não seja aceitável, é necessário avaliar todas as premissas consideradas e seguir para o melhoramento das medidas de proteção.

A metodologia SRAM destina-se a legisladores a nível nacional. As interdependências e riscos intersectoriais não são mencionados nesta metodologia, isto porque esta se orienta para proteção de ativos e ataques terroristas. Apesar da resiliência ser um dos objetivos desta metodologia, não é implicitamente mencionada (Giannopoulos *et al.,* 2012).

2.4.18 Estrutura de Gestão de Risco do Plano Nacional Proteção de Infraestruturas (NIPP)

O pilar da NIPP é a Estrutura de Gestão de Risco, desenvolvida pelo DHS, nos Estados Unidos "…*é a sua estrutura de gestão de riscos que estabelece os processos para combinar informações relativas a consequências, vulnerabilidades e ameaças, de forma a produzir uma avaliação abrangente, sistemática e racional, do risco nacional ou sectorial".*

A metodologia NIPP, que tem em consideração todos os sectores, pretende oferecer uma estrutura que permita disponibilizar recursos de proteção, de forma a reduzir as vulnerabilidades, dissuadir ameaças e diminuir as consequências de ataques e outros acidentes. Isto, tendo em conta as prioridades, metas e requisitos nacionais para infraestruturas críticas. A estrutura de gestão de riscos consiste nas seguintes etapas (DHS, 2017):

- Definição de metas/objetivos;
- Identificação de ativos, sistemas, redes e funções;
- Avaliação de riscos;
- Priorização de riscos;
- Validação de ações de proteção;
- Medidas de redução de risco.

A base teórica é uma estrutura de avaliação de risco clássica, que responde aos sectores de infraestruturas críticas identificadas na Diretiva do DHS – 7 (HSPD-7), ponto 2.3.2. Esta estrutura aborda as considerações físicas, cibernéticas e humanas necessárias para a implementação efetiva de programas abrangentes (Giannopoulos *et al.,* 2012).

A análise resulta numa estimativa de riscos e na validação de medidas de proteção, traduzidas em planos com as principais iniciativas, metas e medidas necessárias para a redução do risco (DHS, 2017).

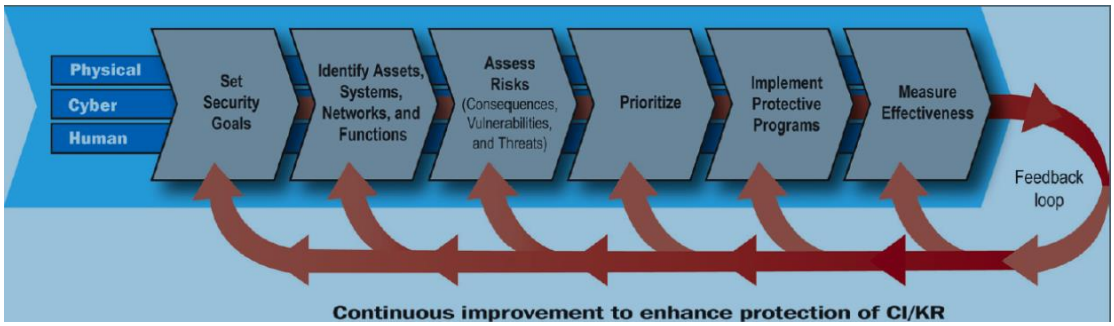


Figura 10 - Estrutura de Gestão de Risco do Plano Nacional Proteção de Infraestruturas (Giannopoulos *et al.*, 2012)

O grupo alvo desta estrutura, ilustrada na Figura 10, são os decisores de entidades federais, como o Departamento de Segurança Interna, estatais, locais, tribais e do sector privado, dos Estados Unidos. A resiliência não é abordada nesta metodologia (Giannopoulos *et al.*, 2012).

2.4.19 Gestão de Riscos de Sectores de Infraestruturas Críticas (GRSIC)

A estrutura de gestão de riscos desenvolvida no Canadá promove a colaboração, de forma a melhorar a resiliência das infraestruturas. Esta estrutura dirige-se a operadores de infraestruturas críticas e governadores locais (Giannopoulos *et al.*, 2012).

A metodologia promove ações mais coerentes e complementares entre as iniciativas federais, provinciais e territoriais, entre os dez sectores de infraestruturas críticas seguintes: energia e utilidades públicas, financeiro, alimentação, transportes, governo, tecnologia de informação e comunicação, saúde, água, segurança e fabrico (PSC, 2009). Os três pilares da estrutura de gestão de riscos são os seguintes (Giannopoulos *et al.*, 2012):

- Perfis de risco sectoriais a nível nacional;
- Avaliações de risco;
- Guias e ferramentas de gestão de riscos.

As interdependências são consideradas em duas fases. Numa primeira fase são consideradas interdependências nos sectores, entre os ativos/infraestruturas do mesmo sector, e numa segunda fase consideram-se interdependências entre sectores. Tendo em conta esta abordagem é necessário analisar riscos intersectoriais na avaliação de riscos. A metodologia para proceder à avaliação dos riscos não é especificada, no entanto são fornecidas algumas indicações em relação aos elementos considerados na metodologia escolhida (Giannopoulos *et al.*, 2012).

A resiliência não é considerada diretamente, no entanto faz parte da estratégia nacional para proteção de infraestruturas críticas (Giannopoulos *et al.*, 2012).

2.4.20 Gestão de Risco da Associação Portuguesa de Segurança (GRAPS)

A metodologia de gestão de risco proposta pela Associação Portuguesa de Segurança é baseada na ISO 31000, sendo composta por cinco fases (APSEI, 2017):

1. Planeamento;
2. Avaliação de risco;
3. Tratamento de Risco;
4. Monitorização e revisão;
5. Comunicação e consulta.

Na primeira fase são comunicados os objetivos e a estratégia a todos os envolvidos, são identificadas obrigações legais ou normativas, são escolhidos os intervenientes e as suas responsabilidades.

A avaliação de risco, segunda fase, divide-se em três etapas: identificação, análise e apreciação do risco. Nesta fase, o primeiro procedimento deve ser dividir a organização em processos e subprocessos e identificar os fatores de risco (FR), nomeadamente, edifícios, utilidades, área envolvente, entre outros. De seguida, procede-se à análise de criatividade que consiste em identificar os processos que podem ter mais consequências tendo em conta critérios predefinidos, tais como, bem-estar social, período temporal, magnitude, etc. (APSEI, 2017).

Na etapa de identificação de risco identificam-se as ameaças, criando uma lista de ameaças de forma a garantir a uniformização entre os vários intervenientes, avaliam-se as vulnerabilidades (Vn) e com o objetivo de hierarquizar os riscos, é efetuada a estimativa do risco através da atribuição de valores à probabilidade, P do cenário ocorrer e da vulnerabilidade por fator de risco (APSEI, 2017).

O último passo da segunda fase é determinado o risco ($R_{parcial)}$ e vulnerabilidade ($V_{parcial}$) parciais através das a expressões (2.10) e (2.11).

$$V_{parcial} = FR\ x\ (V_1 + \cdots + V_n) \tag{2.10}$$

$$R_{parcial} = P\ x\ \left(V_{parcial}\right) \tag{2.11}$$

A terceira fase consiste no tratamento do risco onde são identificados os riscos para os quais há a necessidade de implementação de medidas que permitam a redução e/ou controlo de riscos.

A quarta e última fase corresponde à monitorização e revisão da análise. A metodologia defende que o processo de gestão de risco é um processo contínuo e dinâmico, por isso considera-se fundamental definir o processo de monitorização e revisão da gestão de risco, identificando os responsáveis e a periocidade da realização da mesma (APSEI, 2017).

A metodologia tem em conta as interdependências nos índices de vulnerabilidade utilizados para calcular a vulnerabilidade e o risco.

2.5 Conclusões

O estado de arte das metodologias foi desenvolvido com o apoio do artigo *Risk assessement methodologies for Critical Infrastructures Protection. Part 1: A state of the Art* (Giannopoulos *et al.,* 2012) e complementado com a consulta de outros documentos disponíveis na literatura. Para cada uma das metodologias expostas nesse artigo foram pesquisadas informações adicionais e mais detalhadas de forma a selecionar as metodologias que se consideram mais interessantes do ponto de vista da presente dissertação. A tabela que se encontra no Anexo A permite analisar, para cada metodologia, os seus objetivos, a que sectores se aplica, que perigos considera, se são abordadas as interdependências e a resiliência e algumas vantagens e desvantagens.

Não foi obtida informação adicional para as seguintes metodologias: CARVER2, CommAspen, a Proteção de Infraestruturas Críticas – Diretriz do Conceito de Proteção, Simulação de Modelação de Infraestruturas Críticas (CIMS), Análise e Modelação da Proteção de Infraestruturas Críticas , Análise e Modelação da Proteção de Infraestruturas Críticas (CIPMA), Multicamadas de Redes de Infraestruturas (MIN) e Gestão de Riscos de Sectores de Infraestruturas Críticas.

No processo de escolha da metodologia a utilizar na presente dissertação teve-se em consideração vários fatores, tais como a existência de ferramentas para a aplicação da metodologia, a facilidade de aplicação e a importância dada pelas metodologias à problemática das interdependências e resiliência, isto porque a gravidade das consequências está relacionada com ambos os critérios. No que respeita as interdependências, p.ex. uma falha no fornecimento de energia provoca consequências

não só no próprio sector, mas em outros sectores de infraestruturas críticas como o abastecimento de água ou o funcionamento de transportes. A resiliência permite diminuir ou mitigar as consequências de eventos adversos, sendo assim considerado um critério importante na presente dissertação.

Metodologias como a Modelo de Operações baseado em Efeitos centrados na Rede (NEMO), Análise Rápida, CARVER2, RAMCAP-Plus, Modelação da Avaliação de Risco da Segurança de Redes (NSRAM) e Sistema de Apoio à Decisão de Proteção de Infraestruturas Críticas (CIP/DSS, apesar de serem metodologias interessantes, consistem em *softwares* que não se encontram disponíveis. No entanto, existem pontos interessantes em cada uma desta metodologias que podem fazer parte da metodologia a implementar na presente dissertação.

O *software* CARVER2 é abrangente e considera pontos importantes no que se refere à avaliação de risco, nomeadamente a resiliência, interdependências e vulnerabilidade, ao contrário da maioria das metodologias que não considera a resiliência. Este é o parâmetro que se realça na RAMCAP-*plus* que desenvolveu expressões que permitem quantificar a resiliência do proprietário e da comunidade. A metodologia RAMCAM-*plus* corresponde a uma das metodologias apresentadas mais interessantes pois encontra-se bem estruturada e é uma metodologia abrangente. Na metodologia Análise Rápida, a aplicação *Fastmap* de mapeamento permite gerar mapas e relatórios de ativos em risco, em tempo real, em caso da ocorrência de um evento, p.ex. inundações, incêndios florestais, tsunamis, etc.

As relações *on/off* possíveis na aplicação da metodologia NEMO seriam um recurso benéfico a redes de abastecimento pois permite analisar o efeito em cascada que um dos elementos da rede pode provocar nos restantes. Ainda nessa metodologia são utilizados *softwares* SIG para mapear análises, como será realizado na presente dissertação.

A metodologia NSRAM tem em conta o comportamento humano, ou seja, p.ex. em caso de avaria, essa metodologia tem em consideração os efeitos do pessoal de reparação ou a indisponibilidade de peças. Por fim, a metodologia CIP/DSS propõe o desenvolvimento de perfis de decisores que têm em conta a natureza subjetiva da avaliação de risco.

Sem recorrer a *softwares* é possível aplicar as metodologias EUROCAM, BIRR e RVA, sendo estas compostas por estruturas de avaliação de riscos muitos semelhantes. Assim, devido à existência de ferramentas para aplicação, escolheu-se a metodologia RVA. No entanto, esta metodologia será apenas utilizada como ponto de partida, visto que será

complementada de forma a melhorar a avaliação de riscos do caso de estudo da presente dissertação.

A metodologia RVA foi complementada com a utilização do ArcGIS que permite um melhor entendimento das consequências de potenciais riscos e ainda, através da identificação de planos que permitem melhorar a resposta da empresa a eventos adversos.

Capítulo 3

Gestão de Risco: Caso de Estudo

Capítulo 3 – Gestão de Risco: Caso de Estudo

3 Caso de Estudo

3.1 Descrição do Caso de Estudo

O caso de estudo escolhido foi a rede de abastecimento de água do concelho de Aveiro. A área da rede em estudo consiste numa parte da rede de abastecimento gerida pela AdRA, sendo que na sua totalidade inclui os concelhos de Aveiro, Albergaria-a-Velha, Estarreja, Ílhavo, Murtosa, Oliveira do Bairro, Ovar, Sever do Vouga e Vagos, que equivale a 1500 km² de área onde reside uma população de cerca de 300.000 habitantes (AdRA, 2017).

A rede, como se pode observar na Figura 11, é composta por 8 pontos notáveis (descrição adotada na rede disponibilizada pela empresa AdRA) localizados em 5 freguesias distintas. O Anexo B corresponde à ampliação do esquema geral da rede, que se coloca na Figura 11.

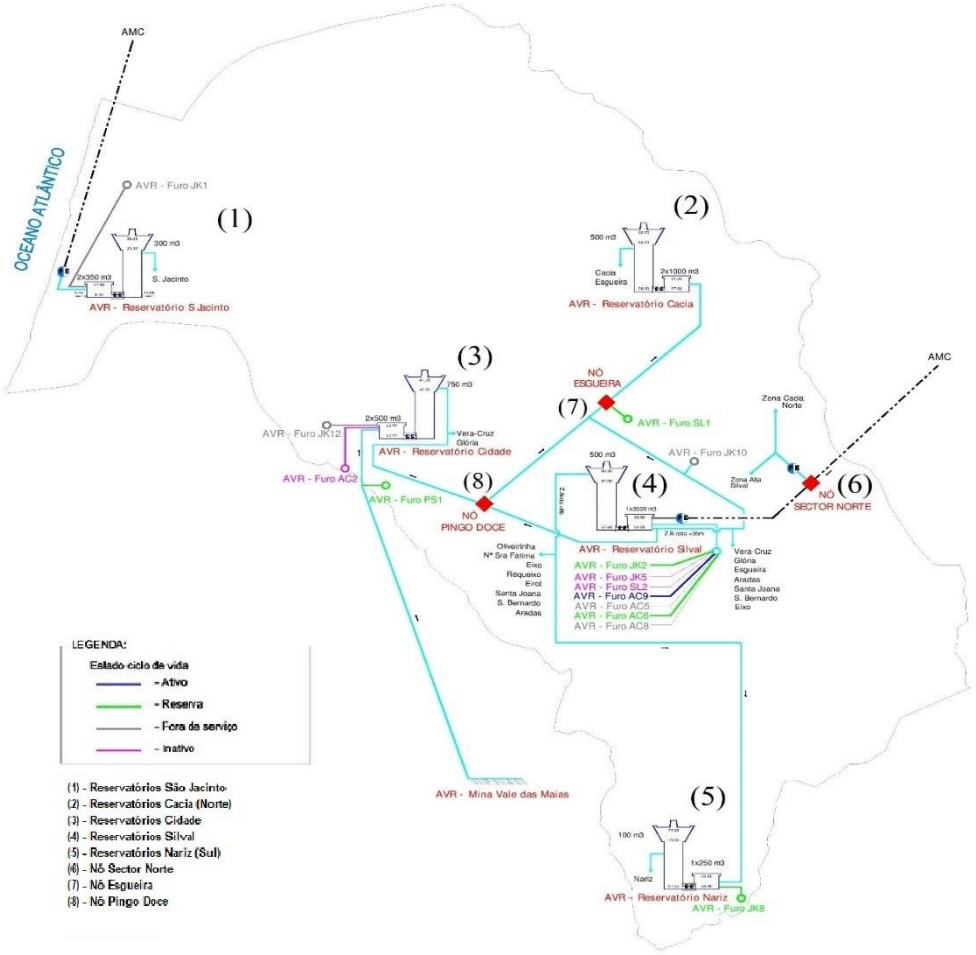


Figura 11 - Esquema Geral da Rede de Abastecimento de Água do Concelho de Aveiro (fornecida pela AdRA)

O primeiro ponto, localizado em São Jacinto, consiste em 3 reservatórios dos quais um é elevado, com capacidade de aproximadamente 300 m³, e dois são apoiados, cada um com

capacidade para 350 m³. Os reservatórios encontram-se ilustrados na Figura 12. Estes reservatórios abastecem a população de São Jacinto que ronda os 1000 habitantes. Note-se que São Jacinto localiza-se no litoral, por isso a população durante a época alta aumenta significativamente.

Figura 12 - Reservatório São Jacinto

Na freguesia de Cacia, localiza-se o ponto notável (2), com 3 reservatórios. Um desses reservatórios encontra-se elevado, com 500 m³ e os restantes encontram-se apoiados com 1000 m³ cada, podendo abastecer as freguesias de Cacia e Esgueira. Este ponto designa-se por Cacia (Norte) e encontra-se na Figura 13.

Figura 13 – Reservatório Cacia (Norte)

No centro da cidade, na freguesia da Glória, situam-se 3 reservatórios. Tal como em Cacia, um dos reservatórios é elevado e dois são apoiados, tendo o primeiro 750 m³ e os restantes 500 m³ cada. As freguesias de Vera-Cruz e Glória podem ser abastecidas por estes reservatórios, identificados como Cidade. Os reservatórios da cidade encontram-se na Figura 14.

Figura 14 – Reservatório Cidade

O ponto notável (4), localizado na freguesia de Oliveirinha, é constituído por 4 reservatórios, um elevado e três apoiados. O reservatório elevado tem capacidade para 500 m³ e dos três apoiados, um tem capacidade para 3500 m³ e dos restantes não se conhece a capacidade, dado que os reservatórios em questão são geridos por uma outra entidade que não a AdRA, a AMC – Associação de Municípios do Carvoeiro. A AMC é responsável pela captação de água no Rio Vouga e distribuição para os centros de distribuição dos concelhos associados, nomeadamente Águeda, Albergaria-a-Velha, Aveiro, Estarreja, Ílhavo, Murtosa, Oliveira do Bairro e Vagos.

Figura 15 – Reservatório do Silval

A Figura 15 representa o ponto notável (4) designado por Silval e permite abastecer quase a totalidade do concelho de Aveiro. O Carvoeiro abastece dois dos reservatórios apoiados que abastecem o terceiro, sendo que este é responsável pelo abastecimento do reservatório elevado. Na Figura 11 é possível verificar que o ponto (4) tem duas saídas diferentes, ou seja, as freguesias de Oliveirinha, Nª Sra. de Fátima, Eixo, Requeixo, Eirol, Santa Joana, São Bernardo e Aradas são abastecidas pelo reservatório elevado, enquanto as restantes freguesias, Vera-Cruz, Glória, Esgueira, Aradas, Santa Joana, São Bernardo e Eixo são abastecidas pelo reservatório apoiado. É necessário notar também que existem freguesias a ser abastecidas por ambos uma vez que as freguesias apresentam locais a cotas diferentes.

A distribuição realizada pelo reservatório do Silval encontra-se dividida entre a Zona Alta, (ZA) que corresponde a locais com altitudes superiores a 35 metros, e a Zona Baixa, (ZB) que corresponde aos locais com altitudes inferiores a 35 metros. O reservatório elevado abastece a Zona Alta e o reservatório apoiado a Zona Baixa.

O ponto Sul, (5) localizado em Nariz, apresenta dois reservatórios, um elevado com capacidade para 100 m^3 e um apoiado com capacidade para 250 m^3. Estes reservatórios, ilustrados na Figura 16, permitem o abastecimento da freguesia de Nariz, no entanto encontra-se inativo, estando vazio, sendo que Nariz é atualmente abastecido pelo Silval.

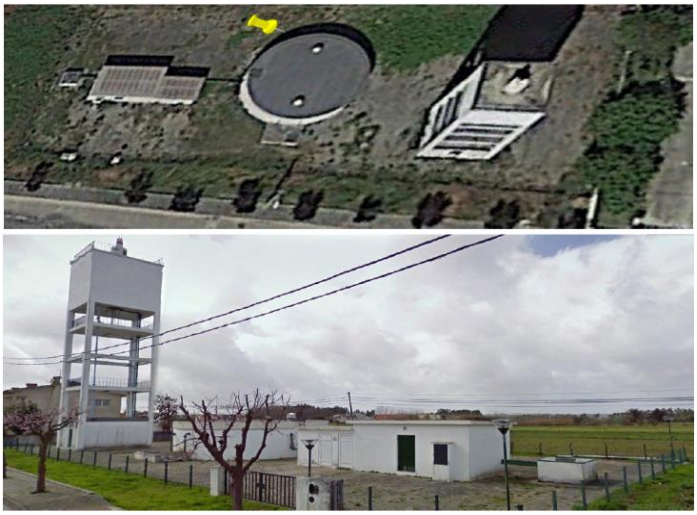


Figura 16 – Reservatórios Sul (Nariz)

Por fim, na Figura 11 é possível observar um sexto ponto designado Nó Sector Norte (6), localizado em Esgueira. Apesar de não existir qualquer reservatório este ponto é considerado notável pois permite reforçar o abastecimento do Silval.

Existem ainda os nós, Nó Esgueira (7) e Nó Pingo Doce (8), localizados respetivamente em Esgueira e Glória. Estes pontos consistem em pontos de manobra e controlo do abastecimento.

3.2 Modelação da Rede de Abastecimento

3.2.1 *Software ArcGIS*

A compreensão integral do funcionamento da rede em estudo é fundamental à gestão de risco. Assim, para melhor compreender e expor esse funcionamento utilizou-se o *software* SIG, *ArcGIS desktop*, da empresa ESRI – *Environmental Systems Research Institute*. Esta ferramenta tem licenças disponíveis para estudantes da Universidade de Aveiro, o que facilitou a sua utilização na presente dissertação.

Os SIG, sistemas de informação geográfica consistem em sistemas destinados ao tratamento automatizado de dados georreferenciados. Estes sistemas manipulam dados de diversas fontes e formatos, dentro dum ambiente computacional ágil e capaz de integrar as informações espaciais temáticas e gerar novos dados derivados dos originais (Assad *et al.,* 1993). O SIG é um sistema informático que captura, armazena, consulta, analisa e exibe dados geoespaciais (Chang, 2017).

O *ArcGIS* fornece ferramentas contextuais para mapeamento e raciocínio espacial para que se possa explorar dados e compartilhar informações baseadas na localização. Cria

uma compreensão mais profunda permitindo compreender onde eventos acontecem e como é que a informação está relacionada. Análise espacial, mapeamento e visualização, SIG 3D, SIG a tempo real, imagens e deteção remota e coleta e gestão de dados são as principais capacidades deste *software* (ESRI, 2017).

Um *shapefile* ESRI consiste num arquivo principal, um arquivo de índice e uma tabela *dBASE*. O arquivo principal é um arquivo de acesso direto, um ficheiro variável-registo-comprimento no qual cada registo descreve uma forma com uma lista dos seus vértices. No arquivo de índice cada registo contém o deslocamento do arquivo principal correspondente, registado desde o início do arquivo principal.

A tabela *dBASE* contém *features atributes*, com um registo por *feature*. A relação um-para-um entre geometria e atributos é baseada no número de registos. Os registos de atributos no ficheiro *dBASE* devem estar na mesma ordem que os registo no arquivo principal (ESRI, 1998).

A análise será realizada no componente do *ArcGIS desktop*, o *ArcMap* que permite exibir e explorar conjuntos de dados GIS, atribuir símbolos e criar *layouts* de mapas para impressão ou publicação. Esta ferramenta permite também criar e editar conjuntos de dados através da caixa de ferramenta (*toolbox*) (ESRI, 2017).

3.2.2 Introdução de dados no *ArcMap*

O *software ArcMap* permitiu analisar e compreender o funcionamento da rede de abastecimento em estudo, que foi disponibilizada pela AdRA, em formato *shapefile*. É de notar que todas as figuras deste ponto correspondem a reduções dos mapas que se encontram no Anexo B. A rede disponibilizada pela empresa incluí os seguintes ficheiros:

- Ventosas;
- Válvulas de suspensão, retenção e descarga;
- Hidrantes e chafariz;
- Pontos de Captação e Entrega;
- Pontos notáveis, descritos no ponto 3.1;
- Nós de Alteração;
- Troços de Tubagem e Adutores;
- Ramais;
- Estações Elevatórias.

Cada um destes ficheiros contém informação adicional, tanto relacionada com características específicas de cada elemento como comum a todos os elementos, nomeadamente a freguesia, a Zona de Monitorização e Controle (ZMC), o estado de operação, o sistema e subsistema.

A análise da rede depende maioritariamente do estado de operação, da freguesia, do sistema e do subsistema. O estado de operação é distinguido entre cadastro, reserva, inativo e fora de serviço. Os sistemas e subsistemas são os reservatórios a que cada elemento está associado, ou seja, o sistema corresponde a reservatório que abastece determinada área em condições normais, enquanto o subsistema corresponde ao reservatório que pode abastecer essa área em caso de necessidade de desativação do sistema, ou seja, funciona como reserva. Por exemplo, um ramal tem como sistema o reservatório da cidade e como subsistema o reservatório da Silval, isto significa que caso o abastecimento através do reservatório da cidade seja interrompido, é possível abastecer este ramal através do reservatório do Silval.

A Figura 17 ilustra a informação disponível sobre a rede de abastecimento, nomeadamente, os pontos notáveis, os pontos de captação, as tubagens e os pontos de entrega juntamente com as tubagens. Os mapas ilustrados na Figura 17 encontram-se no Anexo C.

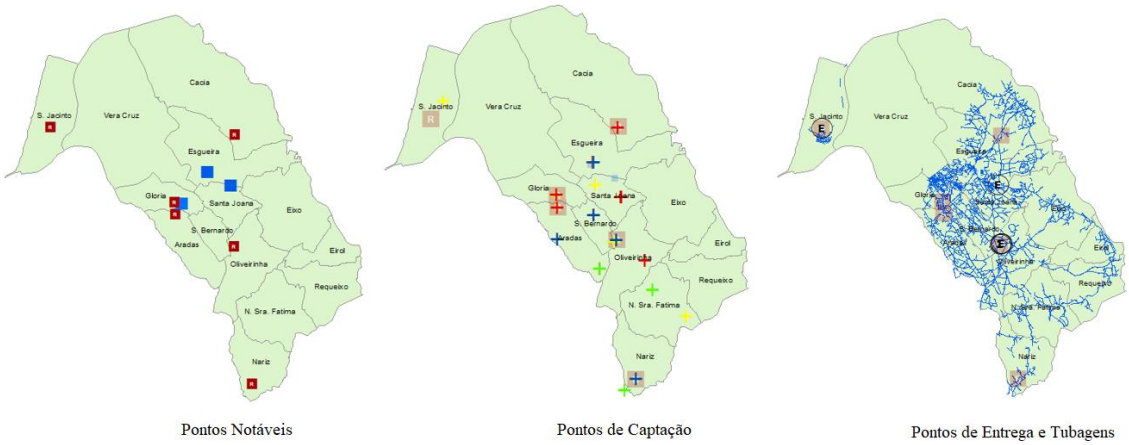


Figura 17 - Elementos da rede de abastecimento

A quantidade de pessoas afetadas pela ocorrência de um evento representa um dos pontos principais na análise e avaliação de riscos. Por esta razão, a informação relativa à população por freguesia do concelho de Aveiro foi obtida através do INE – Instituto Nacional de Estatística. Essa informação é relativa aos Censos 2011 incluindo a

quantidade de residentes total, de residentes mulheres e de residentes homens, de famílias e de edifícios. Na Figura 18 encontra-se a ferramenta utilizada para obter a informação relativa à população.

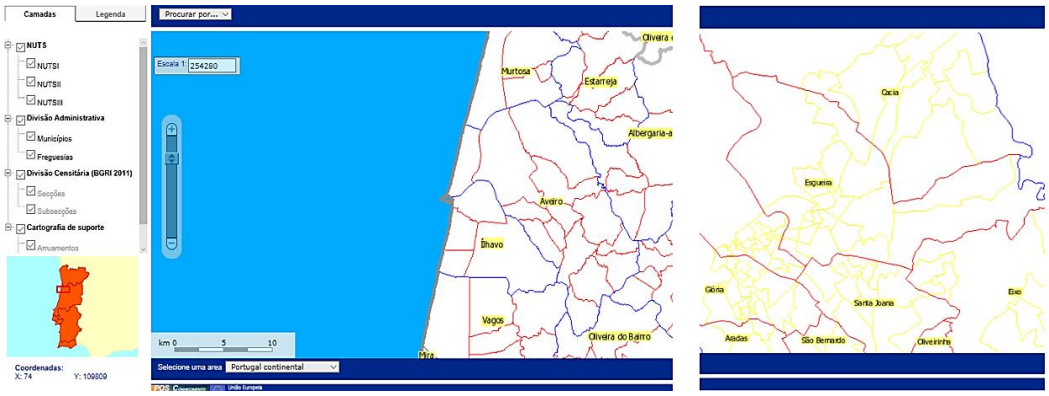


Figura 18 - Ferramenta do INE

Como é possível analisar na Figura 18 é possível distinguir a compartimentação do concelho de Aveiro. As fronteiras vermelhas correspondem às freguesias do concelho enquanto as fronteiras amarelas correspondem a frações de cada freguesia. Para cada uma dessas freguesias foi retirado um *shapefile* que foram depois unidos através da ferramenta *merge*, disponível nas ferramentas de gestão de dados, no *ArcMap*. A Figura 19 corresponde à densidade populacional.

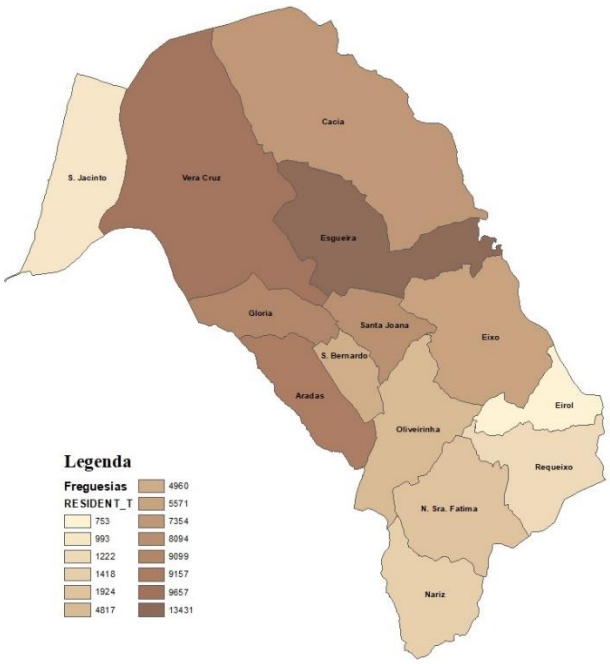


Figura 19 - Densidade Populacional do concelho de Aveiro (fonte CENSOS 2011)

Por fim, foi utilizado o *Google Earth* que permitiu identificar infraestruturas que seriam afetadas por um eventual evento na rede de abastecimento. Essas infraestruturas foram determinadas tendo em conta o Guia Metodológico para a Produção de Cartografia Municipal de Risco e para a Criação de Sistemas de Informação Geográfica (SIG) de base municipal. Foram indicadas infraestruturas relacionadas com Administração Pública, juntas de freguesia e câmara municipal; Equipamentos de Utilização Coletiva, hospitais, centros de saúde, equipamentos de educação, jardins de infância; Equipamentos de Justiça, GNR, PSP, tribunal, bombeiros e lares de 3ª idade; e Infraestruturas Urbanas que correspondem às infraestruturas da rede de abastecimento em estudo.

O locais assinalados são exportados do *Google Earth* em formato KML (*.kml). De forma a importar os locais para o *ArcMap* utilizou-se a ferramenta *From KML: KML to Layer*, disponível nas ferramentas de conversão.

Os locais identificados através do *Google Earth* encontram-se ilustrados na Figura 20. Ao analisar essa Figura 20 verifica-se que existe uma concentração de infraestruturas principais nas freguesias de Glória, Santa Joana e Vera-Cruz, que corresponde ao centro da cidade de Aveiro. Na Tabela 8 é possível analisar a quantidade de infraestruturas principais por freguesia.

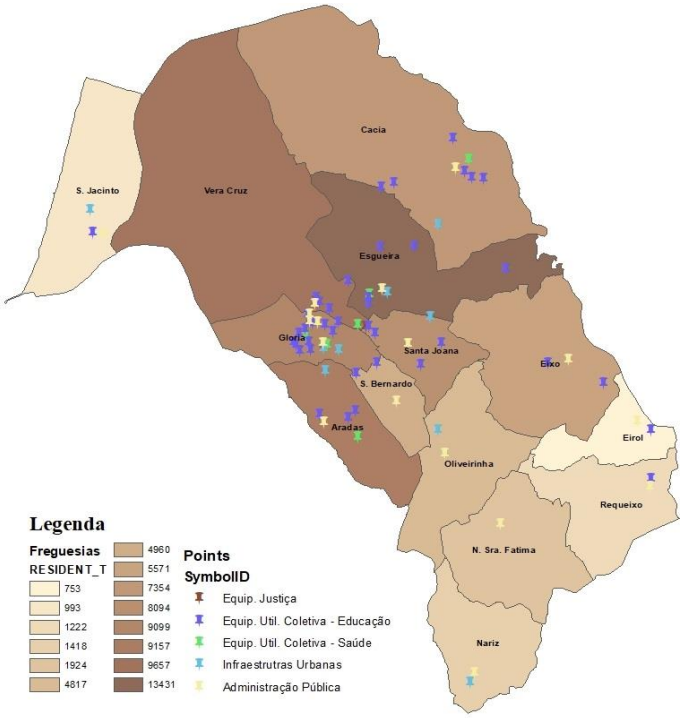


Figura 20 - Locais identificados através do *Google Earth*

Tabela 8 – Quantidade de infraestruturas principais por freguesia

Equipamentos	Aradas	Cacia	Eirol	Eixo	Esgueira	Glória	Nariz
Justiça	0	0	0	0	0	2	0
Educação	3	5	1	2	5	13	0
Saúde	1	1	0	0	1	2	0
Infra. Urbanas	1	1	0	0	1	2	1
Admin. Pública	1	1	1	1	1	4	1
Total	6	8	2	3	8	23	2

	Nº Sra. Fátima	Oliveirinha	Requeixo	Sta Joana	São Bernardo	S. Jacinto	Vera Cruz
Justiça	0	0	0	1	0	0	1
Educação	0	0	1	4	1	1	4
Saúde	0	0	0	0	0	0	1
Infra. Urbanas	0	1	0	1	0	1	0
Admin. Pública	1	1	1	1	1	1	1
Total	1	2	2	7	2	3	7

3.3 Funcionamento da Rede de Abastecimento de Água

Uma rede de abastecimento consiste num sistema complexo com ativos interligados entre si, geridos por entidades que têm como objetivo prestar o melhor serviço aos utilizadores da rede. Assim, quando se analisa o funcionamento de uma rede de abastecimento é necessário considerar o sistema como um todo.

No ponto 3.1 descreveram-se os pontos principais nos quais a gestão de risco se foca. Neste ponto será descrito o funcionamento da rede, identificando os pontos de captação, as interligações entre pontos notáveis, as reservas existentes e como funcionam.

O ponto de captação que permite o abastecimento de água ao concelho de Aveiro localiza-se no Rio Vouga, é designado por Carvoeiro e gerido pela Associação de Municípios do Carvoeiro, AMC. Esta empresa é responsável pelo tratamento de água. Existem 4 pontos de entrega da água abastecida pelo Carvoeiro à rede em estudo, dois deles localizados no Silval, um terceiro no nó Sector Norte e o quarto em São Jacinto. Na Figura 21, retirada do *ArcMap*, é possível ver-se a localização desses pontos de entrega, ilustrados a laranja; é possível também analisar esses pontos de entrega no esquema geral da rede, no Anexo B.

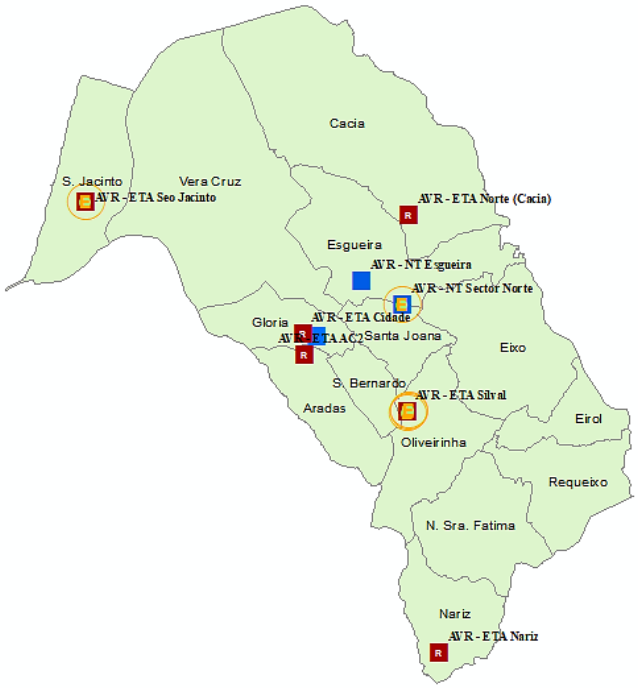


Figura 21 - Pontos de Entrega

No caso de São Jacinto, o abastecimento da população pode ser realizado de duas formas distintas. O Carvoeiro abastece o reservatório elevado que posteriormente abastecerá a população ou abastece diretamente a população de São Jacinto.

A rede de abastecimento de São Jacinto apenas se encontra interligada com a restante rede de Aveiro através da empresa de gestão. Assim, qualquer evento num dos locais, São Jacinto ou na restante rede apenas afetará o outro ao nível da telegestão e apoio ao cliente.

A telegestão, responsável pela monitorização e controlo da rede, encontra-se localizada no Silval, Oliveirinha.

Como já foi mencionado, existem pontos de entrega do abastecimento do Carvoeiro no Silval e no Nó Sector Norte. O Silval é constituído por 3 reservatórios apoiados e um elevado, interligados entre si. O Carvoeiro abastece dois dos reservatórios apoiados que abastecem o terceiro, sendo que este é responsável pelo abastecimento do reservatório elevado. Como já foi explicado no ponto 3.1, o reservatório elevado e o reservatório apoiado abastecem, respetivamente a Zona Alta e a Zona Baixa da cidade de Aveiro.

Ainda relativamente ao Silval, existem neste local saídas de abastecimento que permitem abastecer o Reservatório de Cacia, Nariz e Cidade.

Apesar do abastecimento da rede da cidade de Aveiro ser realizado principalmente pelo Carvoeiro, existem pontos de captação na área da cidade, que estão ativos (cadastro), de reserva, fora de serviço ou inativos. Os pontos identificados como fora de serviço

correspondem a pontos que podem ser ativos, apenas sendo necessário instalar equipamentos como bombas elevatórias. A Figura 22 ilustra a distribuição dos pontos de captação da rede na cidade e os troços adutores que interligam estes pontos aos pontos notáveis.

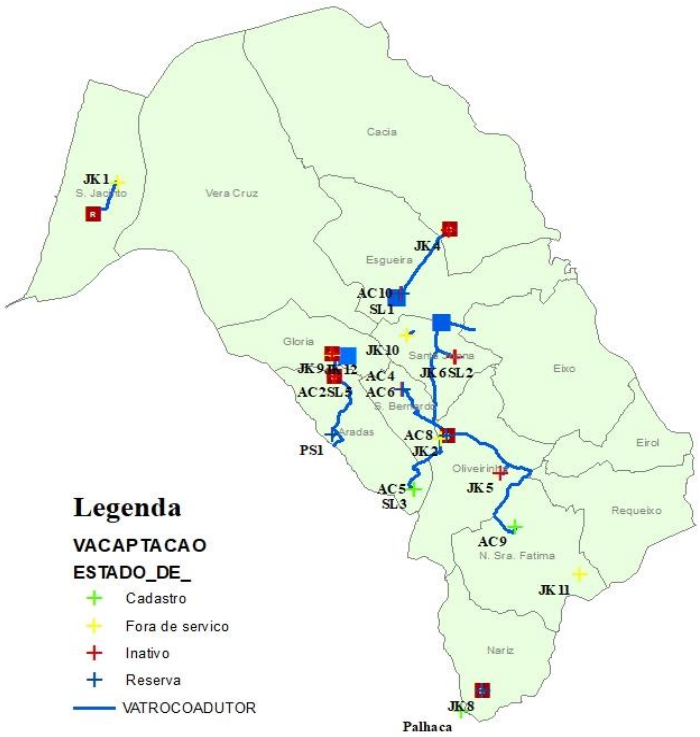


Figura 22 - Pontos de Captação

Como é possível verificar à esquerda, na Figura 22, existe um ponto de captação fora de serviço na freguesia de São Jacinto. A sul existe um ponto que permitem abastecer o reservatório de Nariz, o ponto JK8 identificado como reserva. Não é conhecida a profundidade deste ponto. É de relembrar que o reservatório de Nariz não se encontra em funcionamento. O ponto designado como Palhaça não pertence à rede do concelho de Aveiro, mas sim a um dos concelhos vizinhos, Oliveira do Bairro.

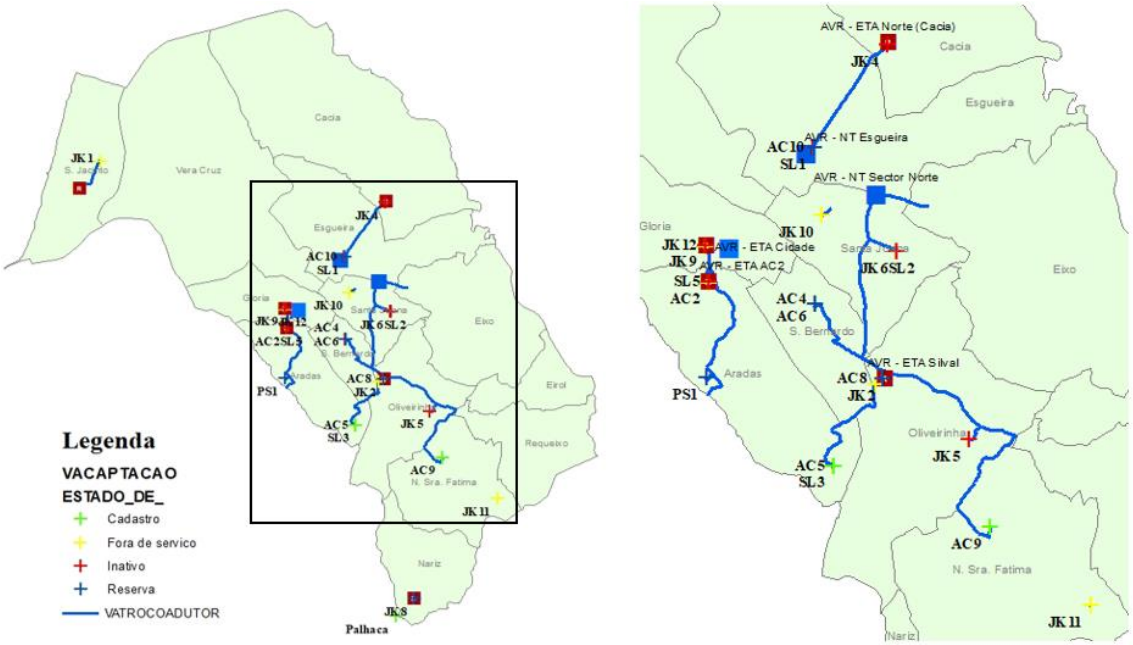


Figura 23 – Ampliação de uma zona da Figura 22

A Figura 23 corresponde à ampliação da zona compacta da rede de abastecimento, que permite uma melhor observação dos dados representados.

A norte, associados aos reservatórios existentes em Cacia – ETA Norte (Cacia), observam-se os pontos JK4 e AC10, ambos inativos, e o ponto SL1 identificado como reserva. De acordo com a rede, existem troços adutores que interligam os três pontos, os reservatórios de Cacia e ainda ao nó de Esgueira.

Os reservatórios da Cidade (ETA Cidade) interligam-se com os pontos de captação JK12, JK9 e PS1 e com a ETA AC 2 associada aos pontos SL5 e AC2. Os pontos JK9 e o AC2 encontram-se inativos enquanto os pontos SL5 e JK12, com profundidades de 265 e 240 metros, respetivamente, encontram-se fora de serviço. Por fim, o ponto PS1 com profundidade igual a 170 metros é identificado como reserva. Existe ainda uma ligação dos pontos associados à ETA Cidade, à Mina Vale das Maias, ilustrada no esquema geral da rede, no Anexo B. Associados aos reservatórios do Silval (ETA Silval) existem cinco pontos inativos: JK5, AC4, AC5, SL2 e JK6; dois de reserva: JK2 e AC6, este com profundidade de 144,96 metros; um fora de serviço, AC8 com 230 metros de profundidade, e dois ativos, AC9 e SL3 com profundidades de 165,88 e 247,50 metros, respetivamente.

Existem ainda dois pontos que não estão interligados com qualquer ponto notável através de troços adutores, no entanto, estão interligados através das tubagens, como é ilustrado na Figura 24.

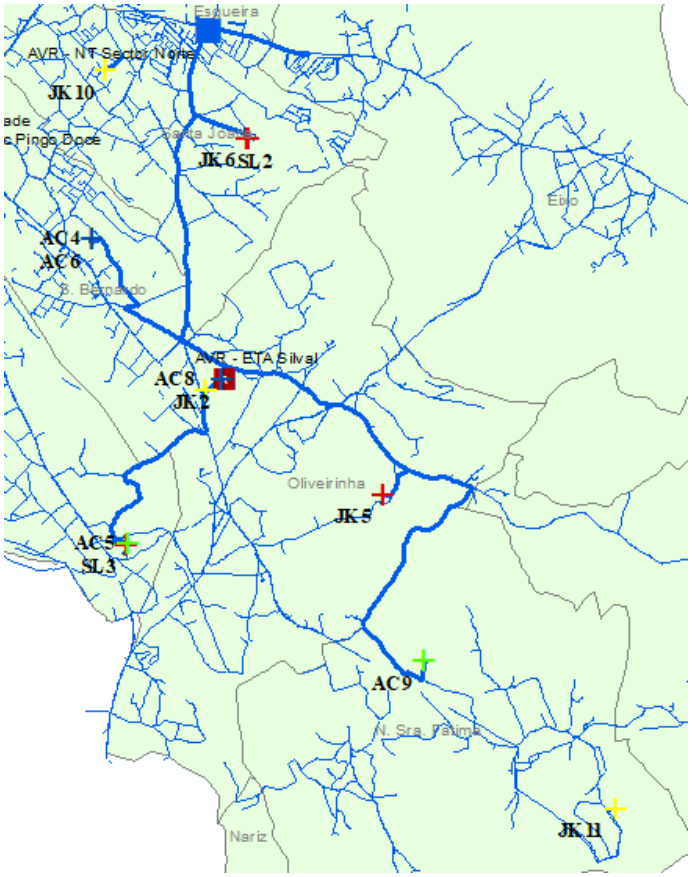


Figura 24 - Pormenor da ligação dos Pontos de Captação JK10 e JK11 à rede

A identificação dos pontos de captação e infomação associada aos mesmos permite proceder à gestão dos recursos disponíveis em caso de ocorrência de um evento indesejado. Isto é, no caso dos pontos fora de serviço é possível desenvolver planos de ação para instalar os equipamentos necessários para que esses pontos deem apoio à restante rede.

Como foi descrito, a rede de abastecimento em estudo pode ser abastecida pelos pontos de captação existentes na rede ou pelo ponto de captação Carvoeiro. O tratamento da água do Carvoeiro é responsabilidade da Associação de Municípios do Carvoeiro, AMC. No caso dos pontos de captação existentes na rede em estudo, a qualidade da água é garantida através de análises realizadas periodicamente.

Nos reservatórios é adicionado à água hipoclorito de sódio a 13% no Silval, Cidade e Cacia e diluído em São Jacinto. O aspecto importante, para a presente dissertação, relativo à adição de agentes desinfetantes, neste caso hipoclorito de sódio, corresponde às bombas doseadoras de hipoclorito de sódio. Isto porque essas bombas não funcionam em caso de falha elétrica ou podem sofrer avarias.

Após a análise dos pontos de captação, um aspecto importante para a gestão de risco corresponde à área de influência de cada ponto notável. Apenas se consideram os pontos notáveis que estão responsáveis pela distribuição, ou seja, os reservatórios de São Jacinto, Cacia, Cidade, Silval e Nariz (desativado).

A área de influência de cada reservatório será visualizada através de mapas exportados do *ArcMap*. A rede disponibilizada contém informações relativas às tubagens da rede e aos ramais, que incluem informação ao sistema e subsistema que lhes está associado. O primeiro mapa, ilustrado na Figura 25, corresponde à área de influência de cada Sistema.

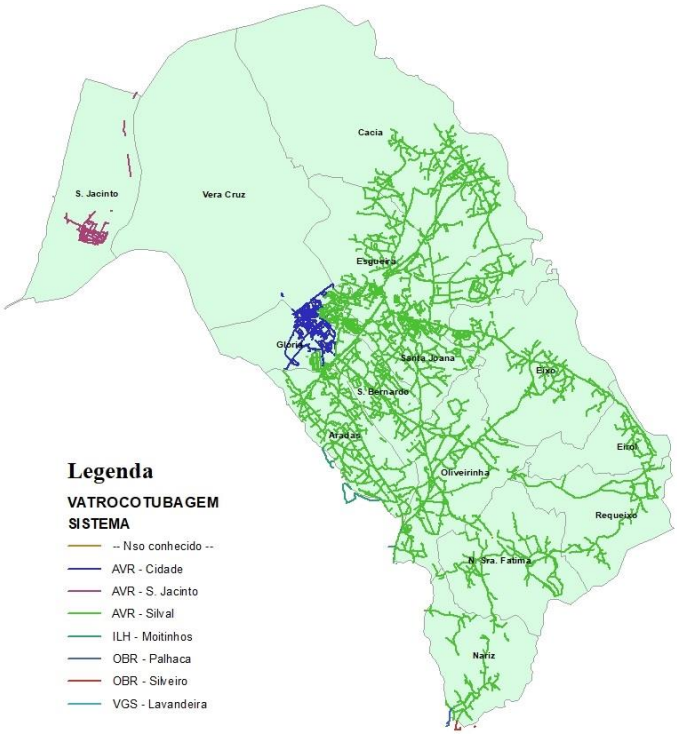


Figura 25 - Área Influência – Sistema

Através da Figura 25 percebe-se que, dos reservatórios em estudo, apenas os da Cidade, São Jacinto e Silval funcionam como sistemas. É possível identificar outros sistemas designados por ILH – Moitinhos, OBR – Palhaca, OBR – Silveiro e VGS – Lavandeira, localizados em Ílhavo (ILH), Oliveira do Bairro (OBR) e Vagos (VGS). Estes locais encontram-se na fronteira do concelho de Aveiro, não estando incluídos na área em estudo. A análise da Figura 25 verifica-se que os reservatórios do Silval têm maior área de influência, resultando num maior número de pessoas afetadas. Na Tabela 9 encontra-se a densidade populacional da área de influência de cada reservatório.

Tabela 9 – Densidade populacional da área de influência dos sistemas

Sistema	População	Freguesias
Silval	63179	Aradas, Cacia, Eirol, Eixo, Esgueira, Glória, Nariz, Oliveirinha, Requeixo, S. Bernardo, Vera Cruz, Santa Joana e Nª Sra. Fátima
Cidade	11428	Aradas, Glória e Vera Cruz
São Jacinto	993	São Jacinto
Moitinhos	2850	Ílhavo

O mapa ilustrado na Figura 26 corresponde aos subsistemas das tubagens e ramais da rede.

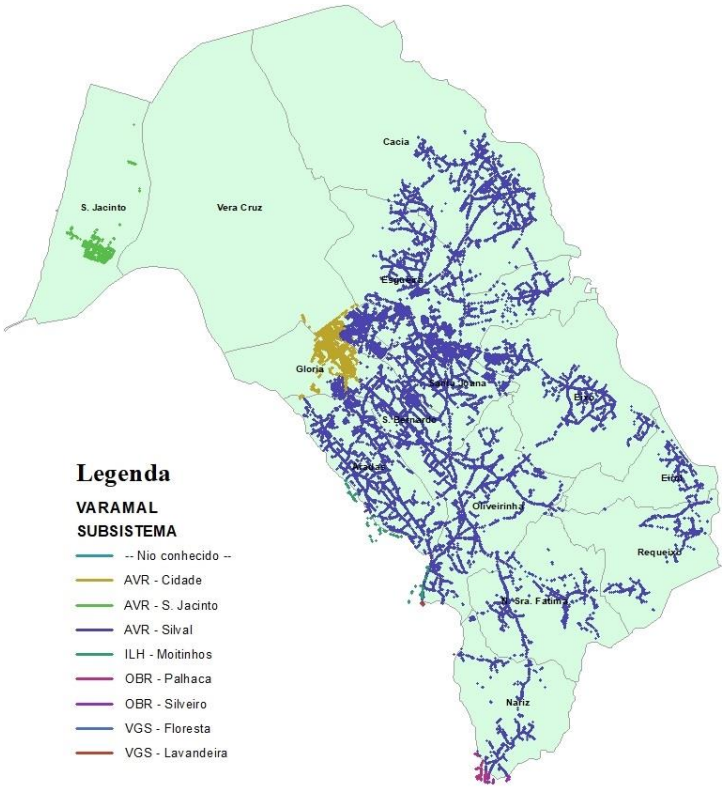


Figura 26 - Área Influência – Subsistema

De acordo com a Figura 26 todos os reservatórios em estudo são subsistemas da rede de abastecimento. Mais uma vez, os reservatórios do Silval têm a maior área de influência. Os reservatórios de Nariz e Cacia permitem abastecer parte da rede, no caso de interrupção do abastecimento do Silval.

Os reservatórios de Nariz têm um ponto de captação de reserva, no entanto os reservatórios encontram-se vazios e não é conhecida a profundidade do ponto de captação. Os reservatórios de Cacia podem ser abastecidos diretamente pelo Carvoeiro através do Nó do Sector Norte.

Encontram-se ilustrados subsistemas que não se têm em conta na presente dissertação: ILH – Moitinhos, OBR – Oil, OBR – Palhaça e VGS – Lavandeira.

Na Tabela 10 é possível analisar a densidade populacional da área de influência dos subsistemas.

Tabela 10 - Densidade populacional da área de influência dos subsistemas

Sistema	Subsistema		População	Freguesias
Silval	Silval	Zona Alta	23940	Aradas, Eixo, Esgueira, Glória, Vera Cruz e Santa Joana
		Zona Baixa	25675	Aradas, Eirol, Eixo, Esgueira, Oliveirinha, Requeixo, S. Bernardo, Vera Cruz, Santa Joana e Nª Sra. Fátima
Cidade	Cidade		11428	Aradas, Glória e Vera Cruz
São Jacinto	São Jacinto		993	São Jacinto
Silval	Norte - Cacia		12146	Cacia e Esgueira
Silval	Sul - Nariz		1418	Nariz
Moitinhos	Moitinhos (Ílhavo)		2850	Aradas e Oliveirinha

No terceiro mapa, ilustrado na Figura 27, será utilizado o *ArcMap* para visualizar a área em que o sistema e o subsistema coincidem, sendo que essas zonas, do ponto de vista de gestão de risco, correspondem às zonas críticas da rede. Isto porque será necessário organizar outras formas para abastecer a área, caso seja necessário.

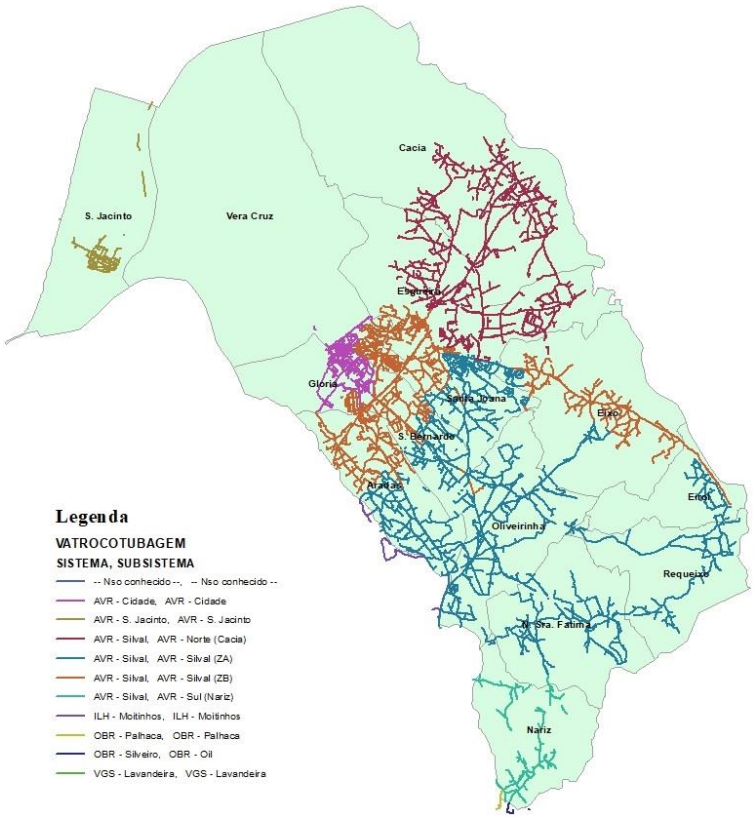


Figura 27 – Área de Influência – Sistema, Subsistema

Apenas as zonas de Cacia e Nariz têm sistemas diferentes dos subsistemas, no entanto, ao contrário do que se visualiza na rede, sabe-se que os reservatórios da Cidade se encontram a ser abastecidos pelo Silval.

Tendo em conta que este (Silval) é o ponto com a maior área de influência e que é utilizado para abastecer outros pontos notáveis, é possível concluir que este é o ponto crítico da rede de abastecimento. Através da Tabela 10, tendo em conta que o ponto Nariz não se encontra ativo, sendo o seu sistema e subsistema o Silval, verifica-se que este afeta 51033 habitantes, o equivalente a 65,1% da população.

A freguesia de São Jacinto, tem também o mesmo sistema e subsistema e apesar de ser possível abastecer a freguesia diretamente através do Carvoeiro, em caso de falha do Carvoeiro, não é possivel abastecer a população. O ponto São Jacinto abastece os 993 habitantes de São Jacinto. No entanto, tendo em conta a sua localização no litoral, na época alta, a população aumenta significativamente.

3.4 Implementação da Metodologia Análise de Risco e Vulnerabilidade (RVA)

A metodologia, descrita no ponto 2.4.16, consiste no preenchimento de quatro *templates* disponíveis em *MSWord* no *site* da DEMA. Esses foram adaptados e traduzidos para português e apresentados no Anexo D.

Será aplicada esta metodologia ao caso de estudo da presente dissertação, a rede de abastecimento de água do concelho de Aveiro.

A DEMA disponibiliza um guia para a aplicação da metodologia que clarifica cada ponto a preencher. Neste guia encontra-se um catálogo de ameaças que foi utilizado para escolher os cenários a desenvolver para o caso de estudo. O catálogo encontra-se no Anexo D. Após a análise desse catálogo decidiu-se desenvolver os seis cenários que se encontram na Tabela 11, integrados em três tipo de incidente/categorias de ameaças distintas.

Tabela 11 – Cenários considerados

Cenário	Título	Categoria de Ameaça/Tipo de Incidente
1	Falha de energia elétrica no ponto do Silval	Destruição ou falha das funções críticas da sociedade
2	Sismo – Intensidade VII	Fenómeno natural extremo
3	Avaria Telegestão	Destruição ou falha das funções críticas da sociedade
4	Avaria de bombas doseadoras de hipoclorito de sódio	Destruição ou falha das funções críticas da sociedade
5	**a)** Ataque cibernético aos sistemas TI (telegestão)	Outras ameaças: Crime
	b) Destruição de um reservatório do Silval	Outras ameaças: Crime
	c) Contaminação da água	Outras ameaças: Crime
6	Falha do Carvoeiro	Destruição ou falha das funções críticas da sociedade

O primeiro, terceiro, quarto e sexto cenários correspondem ao tipo de ameaça destruição, interrupção ou outra falha de funções críticas para a sociedade, sendo o primeiro uma falha elétrica, o segundo avaria na comunicação e sistemas TI (telegestão), o quarto avaria nas bombas de dosagem de hipoclorito de sódio da rede de abastecimento e o sexto corresponde à interrupção do abastecimento de água devido a uma falha no ponto de captação que é externo à rede em estudo e à sua empresa gestora. O segundo cenário que considera a ocorrência de um sismo engloba-se no tipo de ameaça fenómeno natural extremo. O quinto cenário inclui-se em outras ameaças sendo que foram desenvolvidos três cenários, para diferentes tipos de incidentes que são considerados crime.

Os tipos de categorias para os quais não foram desenvolvidos cenários correspondem a ameaças que não se aplicam ao caso de estudo. No ponto 3.4.1 clarificam-se os templates a utilizar na análise. Os *templates* encontram-se preenchidos para cada um dos cenários no Anexo D exceto o *template* 4 que se encontra a seguir no ponto 3.4.9.

3.4.1 Ferramenta de aplicação da metodologia: *templates*

Template 1

O primeiro *template* consiste na identificação da entidade responsável pelo desenvolvimento da avaliação de risco e os participantes na mesma. A entidade responsável considera-se a autora da dissertação, enquanto que os participantes consistem na autora da dissertação e nos professores responsáveis pela orientação da dissertação.

Template 2

O segundo *template* tem como objetivo identificar as ameaças às quais a rede está sujeita e desenvolver um cenário para cada ameaça. O *template* deve ser copiado e preenchido para cada um dos cenários identificados.

Neste *template* são especificadas uma série de condições que devem ser discutidas de forma a desenvolver cenários adequados, tais como:

- Categoria de ameaça/tipo de incidente – desastres naturais, terrorismo, acidentes de transportes, acidentes com substâncias perigosas/poluentes, incêndios e explosões, doenças e epidemias e interrupção/falha de infraestruturas críticas;
- Extensão geográfica – local, regional, nacional, internacional;
- Duração – dias, semanas, meses ou anos;
- Localização no tempo – época do ano e altura da semana;
- Tipo de aviso – sem aviso, curto período de aviso, longo período de aviso;
- Informação de acontecimentos passados – incidente observado no próprio setor, no país, no estrangeiro ou imaginado;
- Causas diretas que levam à realização do cenário – fatores naturais, ações humanas intencionais e não intencionais, defeito técnico ou erros organizacionais.

No *template* 2 pretende-se ainda resumir os eventos e identificar pessoas e ativos afetados.

Template 3

A terceira parte da aplicação da metodologia consiste em cinco secções: A, B, C, D e E nas quais será avaliada a probabilidade de ocorrência do cenário, as suas consequências e as vulnerabilidades dos ativos. Neste ponto serão esclarecidas as secções a desenvolver neste *template*.

1º. **Secção A**: Identificação das funções críticas que a organização tem que manter em caso de ocorrência do cenário em estudo.

2º. **Secção B**: Avaliação da probabilidade de ocorrência do cenário, através dos índices da Tabela 12.

Tabela 12 – Índices de avaliação da probabilidade

1	Altamente improvável
2	Bastante improvável
3	Provável
4	Bastante provável
5	Altamente provável

Para essa avaliação é sugerido ter em consideração a frequência, tendo em conta experiências passadas e a plausibilidade da ocorrência do cenário.

3º. **Secção C:**

1. Identificação das consequências para a organização/área de responsabilidade, particularmente em: edifícios e instalações importantes, pessoal e gestão, sistema TI, fornecimento de energia, acesso a materiais, bens e serviços essenciais, transporte e distribuição, e informação e comunicação;
2. Determinar um nível de consequência geral que corresponde ao maior dos níveis considerados no ponto 1;
3. Avaliação das consequências para a sociedade em geral, nomeadamente: perdas de vida ou saúde, perdas de ativos, ânimo da população ou implicações políticas e interrupção de infraestruturas críticas;
4. Idêntico ao ponto 2;
5. Avaliação geral das consequências.

A cada um dos pontos a preencher na secção C é determinado um nível de consequência através dos índices da Tabela 13.

Tabela 13 - Índice de avaliação do nível de consequência

1	Limitado
2	Moderado
3	Sério
4	Severo
5	Crítico
	Não relevante
	Não se sabe

4º. **Secção D:** Determinação do nível de risco, apresentados na Tabela 14, através da multiplicação dos índices considerados na secção B e no ponto 5, da secção C.

Tabela 14 - Índices de avaliação do nível de risco

1	Risco muito baixo	**9**	Risco médio
2	Risco muito baixo	**10**	Risco médio
3	Risco muito baixo	**12**	Risco médio
4	Risco baixo	**15**	Risco elevado
5	Risco baixo	**16**	Risco elevado
6	Risco baixo	**20**	Risco muito elevado
8	Risco médio	**25**	Risco muito elevado

5º. **Secção E:** Avaliação da vulnerabilidade da organização considerando a preparação antes da ocorrência do evento, através de planeamento e medidas de mitigação, capacidade de resposta e alívio durante e capacidade de recuperação após o incidente.

1. Identificação de medidas de preparação através de planeamento, nomeadamente, planos de reparação geral, ação, segurança e contingência, estratégia para comunicação de crises, educação de pessoal relevante à gestão de crises, entre outros;
2. Identificação de medidas de preparação através de medidas de mitigação, nomeadamente, segurança de ativos;
3. Avaliação geral das preparações existentes para antes do incidente;
4. Análise das capacidades de resposta e alívio e capacidades de recuperação, respetivamente durante e após o incidente, considerando aspetos como gestão, pessoal, equipamentos, organização, logística, entre outros;

5. Avaliação geral das capacidades de resposta e alívio e das capacidades de recuperação.

A avaliação descrita nos pontos 3 e 5 é realizada através dos índices que se encontram na Tabela 15.

Tabela 15 – Índices de avaliação da preparação, capacidade de resposta e alívio e capacidade de recuperação

1	Adequado
2	Predominantemente adequado/Algumas falhas
3	Algumas falhas graves
4	Muitas falhas graves
5	Inadequada
	Não relevante
	Não se sabe

Template 4

No *template* 4, na secção A, identifica-se a entidade para quem se desenvolveu a gestão de risco, as funções críticas nas quais a gestão de risco se foca e, por fim, indica-se a razão para o desenvolvimento da análise, nomeadamente uma nova análise, uma atualização, um requerimento legal, mudanças radicais de ameaças ou mudanças organizacionais.

As secções B e C correspondem respetivamente, à matriz de risco e a uma visão geral da vulnerabilidade da organização.

3.4.2 Determinação da Duração da Água Armazenada nos Reservatórios

O intervalo de tempo no qual é possível abastecer a população através da água armazenada nos reservatórios, ou seja, sem estes estarem a ser abastecidos pelos pontos de captação, é uma informação essencial no que respeita à gestão de crises. Esse intervalo de tempo corresponde ao tempo que a empresa gestora tem para resolver o problema que impede o abastecimento dos reservatórios.

A AdRA disponibilizou os caudais de consumo e nível dos reservatórios elevados e apoiados referentes ao mês de maio. Os caudais de consumo foram disponibilizados para os pontos Silval, Nariz, Cacia e Cidade. Não foram obtidos dados para São Jacinto pelo que será considerado o consumo de Nariz visto que o número de habitantes não difere significativamente.

Os dados disponibilizados incluem aproximadamente quatro leituras por hora com as quais foram determinadas as médias de cada hora e, posteriormente, as médias de cada hora por dias úteis (DU) e fins de semana e feriados (FS/F), tendo-se obtido os respetivos perfis. Estes dados permitem determinar os caudais máximos e mínimos para cada ponto, em dias úteis e aos fins de semana e feriados. Os gráficos das Figura 28, Figura 29, Figura 30 e Figura 31 correspondem aos dados obtidos, respetivamente para os pontos Silval (Oliveirinha), Nariz, Cacia e Cidade.

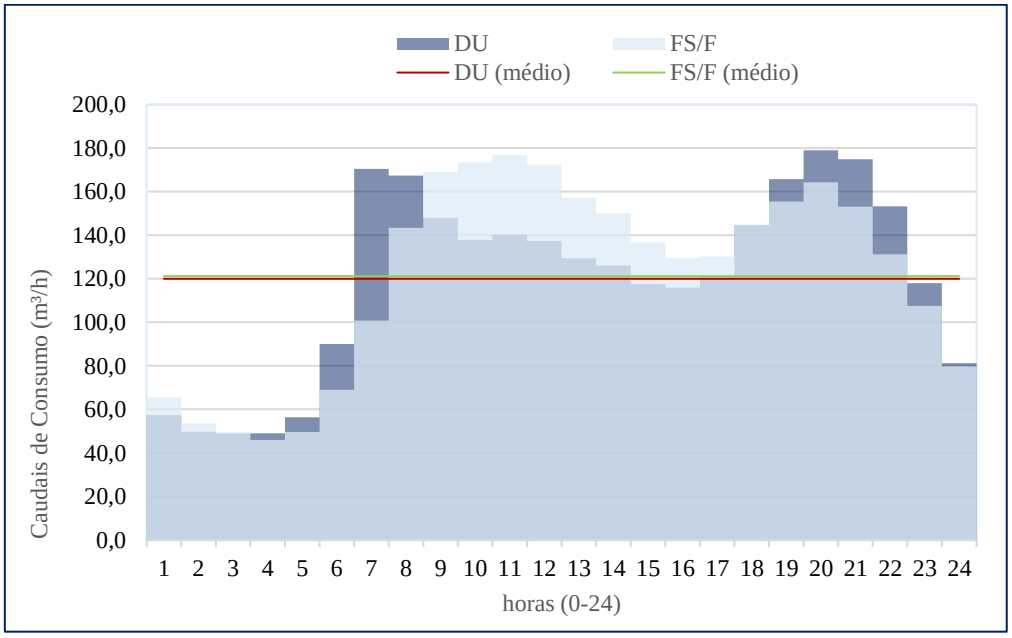


Figura 28 - Perfis de consumo - Silval (Oliveirinha)

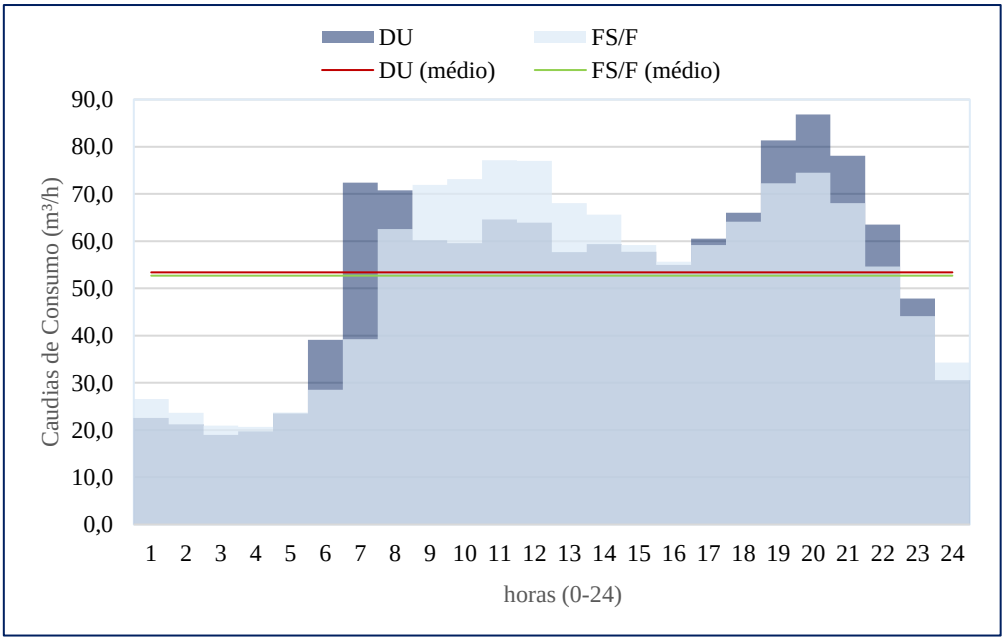


Figura 29 - Perfis de Consumo - Nariz (Sul)

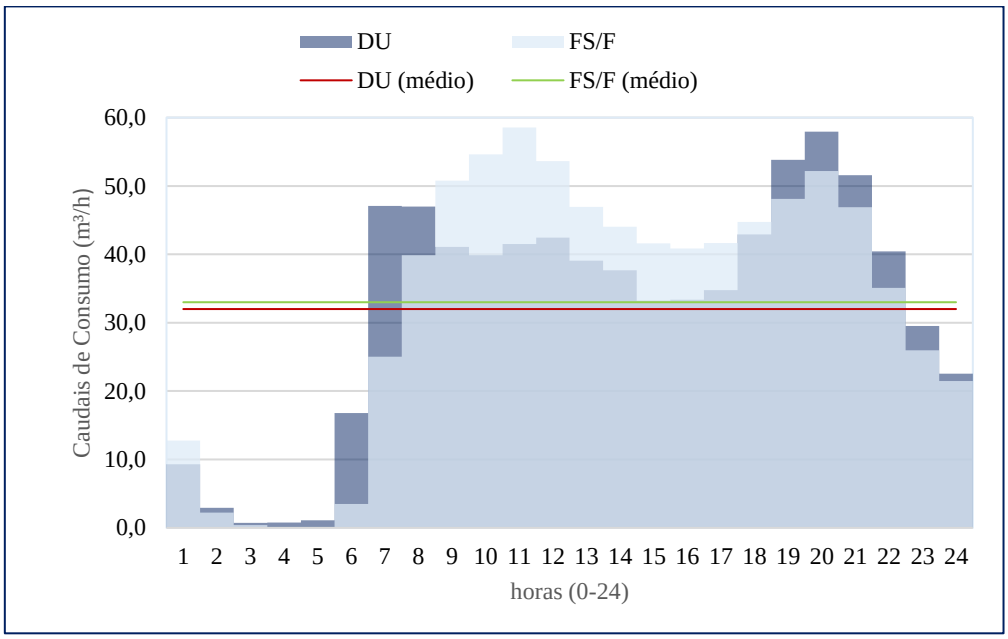


Figura 30 - Perfis de consumo - Cacia (Norte)

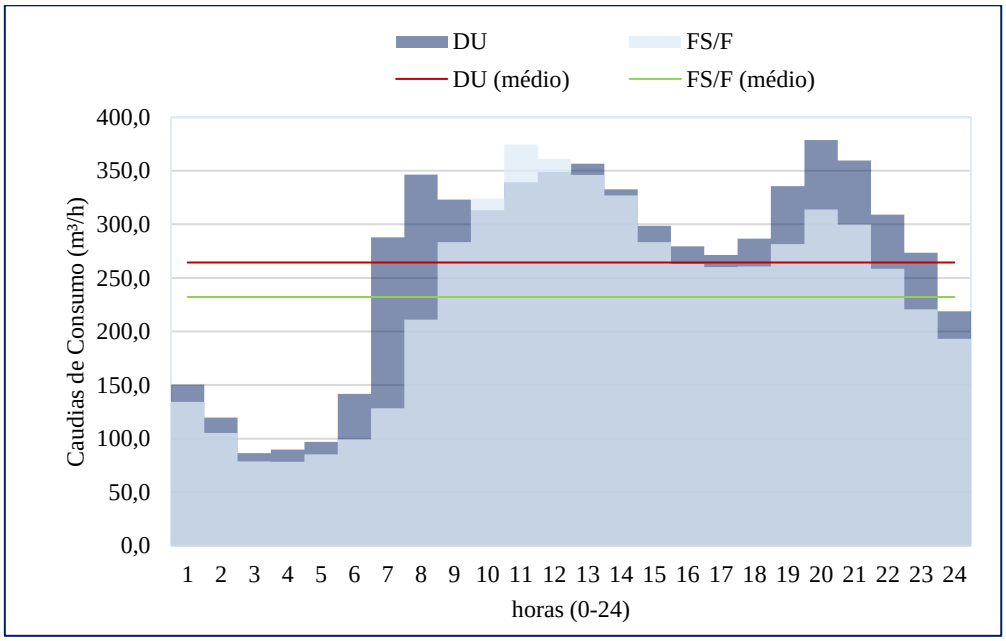


Figura 31 - Perfis de consumo - Cidade

A duração da água nos reservatórios será determinada para os valores médios de caudais de consumo e para os níveis de água nos reservatórios, máximos e mínimos, ilustrados respetivamente na Tabela 16 e Tabela 17.

Tabela 16 - Valores médios dos caudais de consumo

Reservatório		**m³/h**
Cacia		32,0
Silval	**ZA**	58,0
	ZB	62,0
Nariz		53,4
Cidade		264,4

Tabela 17 - Níveis do nível da água dos reservatórios

Reservatório Elevado	
máximo	97,9 **%**
mínimo	67,1 **%**
Reservatório Apoiado	
máximo	93,7 **%**
mínimo	62,9 **%**

As durações mínimas e máximas determinadas para os cenários encontram-se respetivamente, na Tabela 18 e Tabela 19.

Os gráficos apresentados nas Figura 28, Figura 29, Figura 30 e Figura 31 que permitem a análise dos caudais de consumo ao longo do dia, facilita a compreensão da hora do dia a que a ocorrência do incidente seria mais problemática. Por exemplo, ao analisar as durações máximas na Tabela 18 percebe-se que durante o cenário 5 b) é possível abastecer a ZA, ZB e Nariz durante 18,9 horas e, após esse tempo, é possível abastecer ZA e Nariz durante 4,4 horas. No entanto, se o intervalo de tempo 4,4 ocorrer a partir das 19 horas o consumo é mais elevado que a média e, por isso, a água do reservatório durará menos tempo.

Tabela 18 - Durações mínimas

	Níveis de Água nos Reservatórios - Mínimo							
Cenário	**Reservatório**		**Capacidade**	**A abastecer**	**Caudais de Consumo**		**Duração**	
			(m³)		**(m³/h)**	**(m³/h*24)**	**(dias)**	**(h)**
1	Silval	E	335,5	ZA e Nariz	111,4	2672,5	0,13	3,0
5 b)	Silval	A	2201,5	ZA, ZB e Nariz	173,4	4161,7	0,53	12,7
		E	335,5	ZA e Nariz	111,4	2672,5	0,13	3,0
2 e 6	Silval	A	2201,5	ZA, ZB e Nariz	173,4	4161,66	0,53	12,7
		E	335,5	ZA e Nariz	111,4	2672,47	0,13	3,0
	Cacia	A+2E	1593,5	Cacia	32,0	767,52	2,08	49,8
	Cidade	A+2E	817,75	Cidade	264,4	6345,17	0,13	3,1
	São Jacinto	A+E	641,60	São Jacinto	53,4	1281,21	0,50	12,0

Tabela 19 - Durações máximas

Cenário	Níveis de Água nos Reservatórios - Máximo							
	Reservatório		Capacidade	A abastecer	Caudais de Consumo		Duração	
			(m^3)		(m^3/h)	(m^3/h*24)	(dias)	(h)
1	Silval	E	489,5	ZA e Nariz	111,4	2672,5	0,18	4,4
5 b)	Silval	A	3279,5	ZA, ZB e Nariz	173,4	4161,7	0,79	18,9
		E	489,5	ZA e Nariz	111,4	2672,5	0,18	4,4
2 e 6	Silval	A	3279,5	ZA, ZB e Nariz	173,4	4161,66	0,79	18,9
		E	489,5	ZA e Nariz	111,4	2672,47	0,18	4,4
	Cacia	A+2E	2363,5	Cacia	32,0	767,52	3,08	73,9
	Cidade	A+2E	1202,75	Cidade	264,4	6345,17	0,19	4,5
	São Jacinto	A+E	949,60	São Jacinto	53,4	1281,21	0,74	17,8

3.4.3 Cenário 1 – Falha de Energia Elétrica no ponto Silval

3.4.3.1 Introdução

Uma falha elétrica pode ter origem em várias causas, nomeadamente desastres naturais, ações intencionais humanas, ações acidentais humanas ou defeitos técnicos. Apesar dessas causas serem exteriores à rede, esta é afetada pela falha. Numa rede de abastecimento de água as bombas elevatórias, telegestão e estações de tratamento de água dependem da energia elétrica. Sem estes equipamentos pode haver a necessidade de interromper o abastecimento pelo que se considera que a categoria de ameaça/tipo de incidente é a interrupção/falha das funções críticas.

Tendo em conta que se pretende desenvolver o cenário mais desfavorável foram estimadas as durações das reservas dos reservatórios, no ponto 3.4.2, para estabelecer a duração do evento superior ao resultado obtido. As estimativas serão determinadas para o consumo máximo e mínimo, permitindo assim conhecer o intervalo de duração das reservas dos reservatórios.

A falha elétrica afeta ainda as bombas doseadoras do hipoclorito de sódio adicionado à água com o intuito de a desinfetar.

3.4.3.2 Análise do Cenário

Ao analisar os efeitos de uma falha elétrica no ponto notável Silval que provocasse a interrupção do abastecimento de água de pelo menos uma semana, para além da duração das reservas, notou-se que essa falha teria um grande impacto na cidade de Aveiro.

O corte de energia provocaria a interrupção do abastecimento à Zona Alta da cidade, que depende de bombas elevatórias, à área de influência do ponto Nariz, que se encontra inativo e ainda, a impossibilidade de acesso a informação em tempo real da rede, tendo em conta que a telegestão se encontra localizada no ponto Silval e controla e monitoriza toda a rede do concelho de Aveiro. Os resultados da análise encontram-se na Tabela 20.

Tabela 20 - Resultados avaliação - Cenário 1

Probabilidade	1 – Altamente Improvável
Consequência Geral	4 - Severo
Risco	4 - Risco baixo
Preparação	2 – Pred. Adequado/poucas falhas
Cap. Resposta e Alívio	4 – Muitas carências
Cap. Recuperação	1 - Adequado

Assim, ainda que as consequências de uma falha elétrica sejam severas, deve ser considerado que o ponto Silval dispõe de um gerador que permite garantir o fornecimento de energia, de forma a prevenir o evento em estudo.

No entanto, a análise desenvolvida tem em consideração a ocorrência de um evento de cada vez. Apesar da probabilidade de incidentes ocorrerem simultaneamente ser muito baixa, é necessário considerar todos os cenários, mesmos os mais improváveis para que a empresa esteja preparada, mitigando as consequências do evento.

No cenário em estudo, que procedimentos se seguiriam caso o gerador não se encontre operacional? Caso se trate de uma avaria seriam feitos esforços para consertar o gerador, esses esforços, segundo a AdRA podem ter a duração de 6 a 12 horas. No caso de ser necessário substituir o gerador, a substituição do mesmo levaria, segundo a AdRA, aproximadamente 6 horas. Ao ponderar as duas opções é necessário fazer um estudo tendo em conta a demora do arranjo ou substituição e o custo dos mesmos.

A resiliência é um aspeto muito importante na gestão de crises, tendo em conta que corresponde à capacidade de superar e recuperar de adversidades. No caso do presente cenário, pode considerar-se o ativo resiliente a uma falha elétrica visto que o gerador supera essa falha.

3.4.4 Cenário 2 – Sismo

3.4.4.1 Introdução

Os sismos são o resultado de uma libertação súbita de energia, que se propaga sob a forma de ondas sísmicas. A maior parte dos sismos são de origem tectónica, isto é, resultam da libertação de energia quando dois blocos se deslocam ao longo de uma falha, depois de terem sido submetidos à ação de forças. Após atingir o seu limite de elasticidade, isto é, ultrapassado o limite de resistência à deformação, o material entra em rutura, libertando a energia acumulada. Os sismos podem também ser o resultado de abatimentos de cavidades, de explosões produzidas pelo Homem, de deslocamento de magma, entre outros (LNEC, 2017). Anualmente, largas centenas de sismos são registados no território de Portugal Continental, quase todos impercetíveis ao homem (PCL, 2017). Assim, o segundo cenário consiste na ocorrência de um sismo que afetará a rede de abastecimento de água.

O risco sísmico no continente é elevado, sendo que as maiores concentrações demográficas se situam no seu litoral, precisamente nas áreas de maiores intensidades sísmicas observadas na Figura 32.

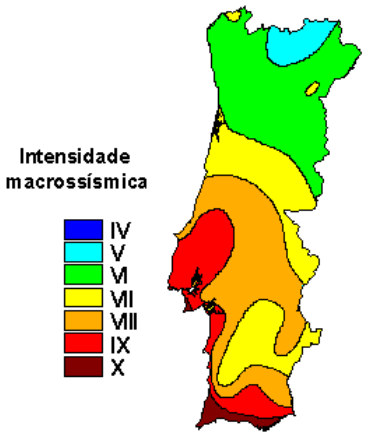


Figura 32 - Intensidade macrossísmica máximo de Portugal (adaptado de LNEC, 2017)

A partir da Figura 32 é possível constatar que Aveiro pode sofrer um sismo com intensidade VII que, de acordo com a escala Mercalli Modificada (IPMA, 2017), corresponde a um grau de intensidade muito forte, que resulta em: dificuldade em permanecer de pé, notado por condutores de automóveis, objetos pendurados tremem, mobílias partem, queda de reboco, tijolos soltos, pedras, telhas, cornijas, parapeitos soltos e ornamentos arquitetónicos, ondas nos tanques, água turva com lodo, pequenos desmoronamentos e abatimentos ao longo das margens de areia e de cascalho, os sinos

grandes tocam e os diques de betão armado para irrigação são danificados (IPMA, 2017). A análise do cenário encontra-se no Anexo C.

3.4.4.2 Análise do Cenário

Um sismo corresponde a um incidente que pode provocar danos ao longo de toda a rede, desde estruturas como os reservatórios, a tubagens que permitem a distribuição da água à população. Por essa razão torna-se impossível determinar exatamente que danos um sismo pode provocar na rede em estudo. Na Tabela 21 encontra-se os resultados da análise realizada para o cenário.

Tabela 21 – Resultados análise – Cenário 2

Probabilidade	3 - Provável
Consequência Geral	4 - Severo
Risco	12 - Risco Médio
Preparação	5 - Altamente Inadequado
Cap. Resposta e Alívio	2 - Predom. Adequado/poucas falhas
Cap. Recuperação	2 - Predom. Adequado/poucas falhas

Visto que não se conhecem as medidas e protocolos da empresa AdRA em casos de emergência, na análise considerou-se que a empresa não tem quaisquer medidas de preparação. Tendo em conta que um sismo consiste num evento que não se pode evitar, devem haver planos de ação que mitiguem as consequências do mesmo.

Nos planos de ação deve analisar-se possíveis danos em todos ativos da rede, podendo em caso de sismo, ocorrer vários incidentes em simultâneo.

Ao ocorrerem incidentes em ativos da rede distintos simultaneamente, devem haver equipas disponíveis para mobilizar aos devidos locais. Caso o incidente provoque mais danos que o previsto, devem existir formas de identificar os locais/ativos de maior importância tendo em consideração o número de pessoas afetadas e as perdas financeiras associadas a cada incidente. Isto permite mobilizar equipas médicas, de segurança e/ou de reparação para os locais mais críticos.

A resiliência no caso de um sismo pode ser determinada tendo em conta o dano que o mesmo provoca em edifícios e elementos da rede. No que respeita a resiliência da rede em estudo não se dispõe de informação suficiente para avaliar, no entanto considera-se que aquando do dimensionamento dos reservatórios a ocorrência de sismos foi considerada, aumentando a resiliência dos mesmos.

3.4.5 Cenário 3 – Avaria Telegestão

3.4.5.1 Introdução

A telegestão encontra-se nas ameaças associadas à comunicação e TI. Estas correspondem, de acordo com o guia da metodologia, a telefones fixos e móveis, processamento e transmissão de dados, redes de informação, acesso a internet, transmissão de TV, satélite e rádio, navegação e correio. Na presente análise será desenvolvido um cenário que tem em consideração uma avaria associada à telegestão, que engloba o processamento e transmissão de dados, redes de informação e acesso à rede.

Os Sistemas de Telegestão (na terminologia anglo-saxónica SCADA - Supervisory Control And Data Acquisition) constituem, atualmente, instrumentos essenciais para uma gestão eficaz dos sistemas de abastecimento de água. Esses sistemas organizados em árvore, numa perspetiva global, podem ser divididos em três níveis hierárquicos: local, zona e supervisão (Sousa, 2003).

A nível local incluem-se as unidades locais que têm, no sistema de telegestão, as funções de aquisição, monitorização, armazenamento de informação, gestão de alarmes e realização de automatismos locais. As unidades locais recebem informação de sensores ou instrumentos de medida, p.ex. medidores de níveis, pressão ou caudais, que processam e armazenam, em parte essa informação, comunicam à unidade de zona os parâmetros relevantes para a operação do sistema e executam automatismos locais, de acordo com as instruções obtidas da unidade de zona (Sousa, 2003).

A unidade de zona gere o subsistema (zona) do sistema de abastecimento de água com base nas instruções da unidade de supervisão e nas informações recebidas das respetivas unidades locais. Para além da gestão técnica e operacional, essas unidades realizam a gestão económica e estatística da zona e gerem as comunicações com as unidades locais. As unidades de zona transmitem para as unidades locais os parâmetros de referência a utilizar nos automatismos locais, p.ex. níveis de fecho e abertura de válvulas de adução, e as ações de controlo a executar nas diversas estações elevatórias ou sobrepressoras incluídas na zona (Sousa, 2003).

Por fim, a unidade de supervisão é instalada num Centro de Despacho que deve dispor de um armário ou frontal de comunicações e, opcionalmente, de um sistema de projeção de sinópticos. Essa unidade recebe informações das unidades locais e de zona e ainda do técnico gestor do sistema.

A unidade de supervisão coordena a gestão efetuada por cada uma das unidades de zona/locais, às quais envia parâmetros e ações de controlo ditadas pela gestão global do sistema (Sousa, 2003).

A organização da telegestão descrita permite que o sistema apresente quatro características que um sistema deste tipo deve ter (Sousa, 2003):

- **Modularidade**, cada unidade é um módulo do sistema;
- **Flexibilidade**, facilidade em alterar a configuração do sistema (acrescentar e/ou retirar unidades);
- **Autonomia local**, cada unidade tem autonomia própria e uma certa independência das restantes unidades;
- **Fiabilidade**, uma avaria numa unidade ou num subsistema não deve implicar a interrupção ou avaria de todo o sistema de telegestão.

Na presente análise será considerada a falha da telegestão por razões variadas, nomeadamente falha elétrica (cenário 1), ataque cibernético (cenário 5, a)) e interrupção do acesso à rede (internet) (cenário 3).

3.4.5.2 Análise do Cenário

A telegestão corresponde a uma ferramenta importante para a gestão diária da rede de abastecimento de Aveiro, pois permite obter informação precisa de forma simples. Por essa razão, a impossibilidade de acesso à mesma pode ter impactos na qualidade do abastecimento, e em caso extremos, consequências físicas na rede.

Na análise desenvolvida considera-se que o acesso à rede é interrompido impossibilitado o acesso à telegestão da rede. Na Tabela 22 encontra-se os resultados dessa análise.

Tabela 22 - Resultados análise - Cenário 3

Probabilidade	3 - Provável
Consequência Geral	4 - Severo
Risco	12 - Risco Médio
Preparação	3 – Algumas falhas graves
Cap. Resposta e Alívio	3 – Algumas falhas graves
Cap. Recuperação	Não se sabe

De acordo com a análise desenvolvida, conclui-se que o nível de risco do cenário 3 é significativo, sendo importante criar medidas que permitam eliminar a ameaça ou mitigar os seus efeitos.

Uma medida que pode mitigar as consequências de uma falha da internet é a realização de acordos com empresas de telecomunicações que permitam a ligação à rede em caso de emergência. Esta medida pode ser considerada uma medida de mitigação, mas pode também eliminar a ameaça, caso a ligação a outra rede seja imediata.

A empresa deve ainda analisar a possibilidade de o acesso à rede ter uma duração muito longa devido à falha geral da internet. Uma falha de longa duração pode causar não só problemas na qualidade do abastecimento, mas também danos físicos. Neste caso, devem ser desenvolvidos planos que ditem como será monitorizada a rede, de forma a garantir a qualidade do abastecimento.

3.4.6 Cenário 4 – Avaria na Rede de Abastecimento – Avaria bomba doseadoras

3.4.6.1 Introdução

No Cenário 4 considerou-se uma avaria da própria rede de abastecimento, a avaria de bombas doseadoras. Como já foi mencionado no ponto 3.1, a rede em estudo é abastecida pelo ponto de captação existente no Rio Vouga, designado por Carvoeiro que é responsável pela qualidade da água. No entanto, nos reservatórios do Silval, Cidade e São Jacinto é adicionado hipoclorito de sódio, de forma a desinfetar a água, que é controlado através de bombas doseadoras. Essas bombas, como já foi mencionado no ponto 3.3, não funcionam sem energia elétrica ou podem sofrer avarias.

O presente cenário foca-se na eventualidade das bombas sofrerem avarias, visto que a falha elétrica foi analisada no Cenário 1 – Falha de Energia Elétrica no ponto Silval. O cenário será desenvolvido para os reservatórios do Silval pois a sua área de influência corresponde quase à totalidade do concelho de Aveiro.

3.4.6.2 Análise do Cenário

A adição de hipoclorito de sódio à água para abastecimento tem como objetivo desinfetar a água, sendo que elimina agentes patogénicos como vírus, bactérias e protozoários, que provocam doenças. Os resultados obtidos na análise desenvolvida para o cenário encontram-se na Tabela 23.

Tabela 23 - Resultados análise – Cenário 4

Probabilidade	4 – Bastante provável
Consequência Geral	3 - Sério
Risco	12 - Risco Médio
Preparação	2 – Predom. Adequado, algumas falhas
Cap. Resposta e Alívio	2 – Predom. Adequado, algumas falhas
Cap. Recuperação	1 - Adequado

Através da análise desenvolvida verifica-se que existe um nível de risco médio associado ao cenário. Assim, é necessário existirem planos de ação que garantam a qualidade do abastecimento, evitando problemas de saúde pública.

Neste cenário considerou-se que a preparação e capacidades da empresa são predominantemente adequadas, visto que no caso de avaria das bombas, a telegestão identifica a avaria e considera a intervenção de reparação da mesma como uma intervenção urgente. Assim, o tempo de resposta à avaria é muito reduzido.

Note-se ainda que os níveis de hipoclorito na água descem gradualmente e não instantaneamente, e sendo o tempo de resposta muito curto, a avaria é reparada antes de afetar a qualidade do abastecimento.

No entanto, deve ser analisada a possibilidade da telegestão não identificar a avaria ou da reparação da avaria demorar um longo período de tempo, havendo a necessidade de interromper o abastecimento de água e garantir a distribuição da água à população de outras formas.

3.4.7 Cenário 5 – Crime

3.4.7.1 Introdução

Segundo o guia de apoio à aplicação da presente metodologia, existem vários exemplos de crime que podem constituir ameaças para as infraestruturas críticas. No caso do presente cenário serão consideradas dois desses exemplos: ataque aos sistemas TI, ou seja, *hacks* ao sistema e vandalismo/sabotagem, que incluí destruição de edifícios ou instalações importantes e contaminação da água.

De forma a analisar ambos os exemplos, serão desenvolvidos três cenários: Cenário 5, a) ataque aos sistemas TI, Cenário 5 b) vandalismo e sabotagem – destruição do reservatório do Silval responsável pela distribuição da água fornecida pelo Carvoeiro aos restantes reservatórios, e Cenário 5 c) vandalismo e sabotagem – contaminação da água.

Nos últimos anos, os ataques cibernéticos contra infraestruturas críticas têm aumentado globalmente. No entanto, a crescente consciencialização não se traduz necessariamente na implementação de melhores protocolos de segurança e sistemas mais seguros (Espelund, 2016).

No setor de água potável um ataque cibernético pode atuar em quatro vertentes diferentes de ameaça: contaminação química, contaminação biológica, interrupção física e interferência com os sistemas de computador altamente especializados que controlam a infraestrutura, designados como sistemas de Controlo Supervisor e Aquisição de Dados, SCADA (Deane, 2003).

Na análise de possíveis ataques cibernéticos à rede não se consideram as contaminações biológica e química pois como já foi mencionado o tratamento da água é responsabilidade da empresa que realiza a captação no Carvoeiro, a Associação de Municípios do Carvoeiro, AMC. Existem nos reservatórios equipamentos de adição de hipoclorito de sódio que desinfeta a água. No entanto, esses equipamentos e as bombas doseadoras não são controlados pela telegestão, sendo a sua configuração realizada manualmente.

A interrupção física consiste em utilizar o sistema de telegestão para interromper o abastecimento de água. Isto pode acontecer se se abrir/fechar válvulas ou desligando uma estação elevatória. Um ataque cibernético pode ter o intuito de interferir na rede através do sistema SCADA, alterando os caudais, pressões, estado de válvulas, entre outros.

No cenário relativo ao vandalismo/sabotagem considera-se a destruição de edifícios ou instalações importantes e contaminação da água. O primeiro pode consistir em incidentes como destruição de bombas elevatórias ou destruição parcial ou total de reservatórios. A água pode ser contaminada provocando a destruição das bombas doseadoras ou equipamentos de adição de hipoclorito de sódio ou introduzindo contaminantes diretamente na água.

O Silval é considerado o ponto crítico da rede devido à sua área de influência e por corresponder a um dos pontos de entrega do abastecimento do Carvoeiro. Assim, o segundo cenário a desenvolver consiste na destruição do reservatório responsável pela distribuição da água fornecida pelo Carvoeiro aos restantes reservatórios que abastecem o concelho de Aveiro. Por fim, o terceiro cenário corresponde à contaminação da água do reservatório do Silval, sendo que não é relevante a forma como foi contaminada visto que ambas as situações descritas requerem presença física.

3.4.7.2 Análise do Cenário

As questões de segurança de redes de abastecimento de água são motivo para preocupação, no entanto até hoje têm recebido menos do que uma atenção adequada (Tularam *et al.*, 2011).

As ameaças a um sistema de distribuição de água podem ser divididas em três grandes grupos de acordo com os métodos necessários para melhorar a sua segurança: ataques diretos às infraestruturas principais, ataques cibernéticos que desabilitam a funcionalidade do sistema de controlo e supervisão e de aquisição de dados (SCADA) da rede e injeção deliberada de contaminantes químicos ou biológicos num dos elementos do sistema (Ostfeld, 2006).

Na Tabela 24 encontram-se os resultados da análise desenvolvida para o cenário de um possível ataque cibernético.

Tabela 24 – Resultados análise – Cenário 5, a).

Probabilidade	1 – Altamente improvável
Consequência Geral	4 - Severo
Risco	4 – Risco Baixo
Preparação	5 – Altamente Inadequado
Cap. Resposta e Alívio	5 – Altamente Inadequando
Cap. Recuperação	4 – Muitas carências

De acordo com a análise realizado o nível de risco do cenário de ataques cibernéticos à rede é baixo e as consequências severas. Isto significa que apesar da probabilidade do cenário ocorrer ser muito baixa, as consequências da sua ocorrência seriam problemáticas podendo resultar na interrupção do abastecimento durante um longo período de tempo.

Assim, a segurança dos sistemas SCADA (telegestão) deve ser analisada e melhorada, se necessário. Note-se que apesar de ser recomendada uma boa segurança dos sistemas, não existem garantias que os ataques não ocorram visto que não existem sistemas 100% seguros.

Algumas medidas que aumentam a segurança dos sistemas são as seguintes:

- controlo de acesso, através de acordos de acesso, implementação de softwares e protocolos de mecanismos de autenticação, *passwords* e autenticação e ID dos utilizadores;
- Auditorias e responsabilização;
- Proteção de comunicações;
- Cópias de segurança do sistema;

- Entre outros.

O segundo cenário relativo ao tipo de ameaça criminalidade, corresponde à destruição do reservatório responsável pela distribuição da água abastecida pelo Carvoeiro para os reservatórios da rede em estudo. Os resultados da análise deste cenário encontram-se na Tabela 25.

Tabela 25 - Resultados avaliação - Cenário 5, b)

Probabilidade	1 – Altamente improvável
Consequência Geral	4 - Severo
Risco	4 – Risco Baixo
Preparação	3 – Algumas falhas graves
Cap. Resposta e Alívio	2 – Predom. Adequado, algumas falhas
Cap. Recuperação	Não se sabe

A destruição do reservatório é considerada altamente improvável, no entanto as consequências do incidente são significativas.

No que toca a preparação, foi considerado que não existem planos de ação por falta de informação. No entanto, planos de ação devem ser desenvolvidos de forma a gerir o incidente e mitigar as consequências do mesmo.

Planos de segurança para garantir a segurança do pessoal empregado pela AdRA devem ser desenvolvidos. Para o caso de interrupções do abastecimento por longos períodos de tempo, podem ser desenvolvidos acordos e planos com outros concelhos para que estes ajudem no abastecimento à população.

Se se prever interrupções prolongadas devem existir planos que indiquem os ativos para os quais o abastecimento deve ser uma prioridade, nomeadamente, equipamentos de saúde como hospitais e centros de saúde.

O cenário trata a destruição dum reservatório. Acordos podem ser feitos com empresas de construção que garantam a reconstrução dos ativos destruídos num curto período de tempo.

Por fim, o terceiro cenário relacionado com a criminalidade é a contaminação da água. Este é um cenário que, em caso de ocorrência, pode causar elevadas perdas de vida e saúde. Os resultados obtidos na análise encontram-se na Tabela 26.

Tabela 26 - Resultados avaliação - Cenário 5, c)

Probabilidade	1 – Altamente improvável
Consequência Geral	5 - Crítico
Risco	5 – Risco Baixo
Preparação	3 – Algumas falhas graves
Cap. Resposta e Alívio	3 – Algumas falhas graves
Cap. Recuperação	Não se sabe

De acordo com a análise o nível de risco de contaminação da água é baixo, no entanto concluiu-se que as consequências desse evento seriam críticas.

No que diz respeito à preparação, existem medidas de mitigação do cenário tendo em conta que a análise da água em tempo real permite à telegestão identificar a contaminação.

Na capacidade de resposta e alívio consideraram-se apenas entidades exteriores à empresa gestora, como serviços dos bombeiros, proteção civil, PSP e GNR. Em termos de recuperação do sistema, não se tem informação se existem capacidades.

No presente cenário é essencial existirem planos para a comunicação da ocorrência à população, de forma a diminuir o número de pessoas afetadas caso seja abastecida água contaminada. Planos dos procedimentos no caso de ocorrência deste evento é também importante, nomeadamente a formação do pessoal ligado à gestão de crises.

A garantia de abastecimento a equipamentos de saúde, principalmente hospitais é uma prioridade tendo em conta que podem existir pessoas contaminadas. A identificação do contaminante é essencial para melhor tratar as pessoas infetadas.

Devem ser desenvolvidos planos para garantir a recuperação rápida do abastecimento de água.

3.4.8 Cenário 6 – Falha do Carvoeiro

3.4.8.1 Introdução

O Carvoeiro é o ponto de captação principal da rede de abastecimento da cidade de Aveiro. Nesta rede existem três pontos de entrega do abastecimento do Carvoeiro, ilustrados na Figura 21, localizados no recinto dos pontos São Jacinto e Cidade e no Nó Setor Norte.

O cenário a desenvolver considera a falha deste ponto de captação sendo que essa pode ser causada por vários fatores distintos tais como fenómenos naturais extremos (deslizamentos de terras, cheias e secas), falha de energia, ataques cibernéticos, contaminação de água, acidental ou intencional (descarga de substâncias

perigosas/poluentes no rio) ou crime. No entanto, para a presente análise não se consideram as causas, mas sim consequência da falha Carvoeiro que corresponde à interrupção do abastecimento do Carvoeiro à rede em estudo.

3.4.8.2 Análise do Cenário

O Carvoeiro consiste no ponto de captação que distribui água à rede de abastecimento em estudo, sendo que esta é significativamente afetada pela falha do Carvoeiro. Para o desenvolvimento da análise a informação relativa ao Carvoeiro é limitada.

A probabilidade considerada para o cenário supõe que existem planos de ação e contingência que visam garantir o abastecimento aos concelhos aos quais esse ponto fornece água. Os resultados da avaliação encontram-se na Tabela 27.

Tabela 27 - Resultados avaliação - Cenário 6

Probabilidade	2 – Bastante improvável
Consequência Geral	5 - Crítico
Risco	10 – Risco Médio
Preparação	4 – Muitas carências
Cap. Resposta e Alívio	5 – Altamente inadequado
Cap. Recuperação	2 – Predom. Adequado, algumas falhas

Apesar de se considerar que o evento é bastante improvável, note-se que as consequências seriam críticas visto que o cenário afeta a totalidade do concelho de Aveiro.

Na avaliação da preparação e capacidades de resposta e alívio a análise realiza-se sem informações relativas às medidas e capacidades que a empresa AdRA possui. As capacidades de recuperação consideram-se altamente inadequadas visto que para a AdRA recuperar totalmente do evento é necessária a recuperação do Carvoeiro.

No ponto 3.3 analisou-se a área de influência de cada um dos sistemas e subsistemas dos reservatórios. Na Figura 27 observa-se que existem zonas da rede nos quais o sistema e o subsistema são o mesmo, nomeadamente a área de influência do Silval, São Jacinto e Cidade.

O ponto Cidade não é afetado pela interrupção do abastecimento do Carvoeiro pois possui capacidade para abastecer sem o fornecimento de água deste. No entanto, os pontos Silval e São Jacinto dependem do abastecimento do Carvoeiro. Os pontos de Nariz e Cacia dependem do Silval e, por consequência, do Carvoeiro. Esta análise permite concluir que

no caso de ocorrência da falha do ponto de captação, apenas se garante o abastecimento na área de influência do ponto Cidade.

De forma a minimizar as consequências da falha do Carvoeiro, nos restantes locais, devem ser identificadas formas de garantir o abastecimento de água para necessidades básicas, p.ex. através de carros de bombeiros abastecidos em concelhos vizinhos. Esse abastecimento deve ter em consideração ativos que são prioritários, como hospitais.

Em caso de ocorrência da falha na época alta (verão) é necessário tem consideração o aumento significativo de habitantes na freguesia de São Jacinto.

Comunicados à população relativa à interrupção do abastecimento e ao incentivo para a poupança de água são medidas a desenvolver.

3.4.9 Perfis de Risco e Vulnerabilidade

O quarto e último *template* da metodologia de avaliação de riscos consiste principalmente no desenvolvimento dos perfis de risco e vulnerabilidade. O primeiro consiste numa matriz de risco que considera a probabilidade de ocorrência de cada cenário e o nível de consequência geral. O perfil de vulnerabilidade consiste numa tabela que permite analisar a vulnerabilidade do caso de estudo nos oitos cenários desenvolvidos. Na Tabela 28 é apresentada a tabela referente ao caso de estudo.

Tabela 28 - Matriz de risco

B: Matriz de Risco						
Probabilidade	Altamente provável (5)					
	Bastante provável (4)			**Cenário 4**		
	Provável (3)				**Cenário 2 e 3**	
	Bastante improvável (2)					**Cenário 6**
	Altamente improvável (1)				**Cenário 1, 5 a) e b)**	**5 c)**
Risco muito elevado						
Risco elevado		Limitado (1)	Moderado (2)	Sério (3)	Severo (4)	Crítico (5)
Risco médio						
Risco baixo						
Risco muito baixo		Consequências				

Na matriz de risco é possível identificar a probabilidade de ocorrência e os níveis de consequência que estão associados a cada cenário. Isto permite hierarquizar a importância de cada um dos cenários, dependendo do que se considera mais significativo, ou seja, caso se acredite que os cenários com níveis de probabilidade (3) (provável) e com consequência (3) (sério) consistem nos mais importantes para a empresa gestora, então o investimento em medidas de preparação e mitigação serão direcionadas prioritariamente para os cenários com essas probabilidades e níveis de consequência.

A matriz de risco permite verificar que os cenários 1, 5 a), b) e c) e 6 apesar de estarem associados a probabilidades baixas, as consequências dos mesmos, em caso de ocorrência, seriam significativas. No que respeita os cenários 2, 3 e 4 verifica-se que são cenários significativos pois ambos têm probabilidade média de ocorrer e as consequências dessa ocorrência podem ser sérias ou severas.

No que respeita à vulnerabilidade da rede de abastecimento em estudo é possível verificar na Tabela 29 que a rede tem vulnerabilidade elevada em caso de ocorrência de alguns cenários. O cenário a que a rede parece ser mais vulnerável é o ataque cibernético, cenário 5 a). É necessário ter-se em conta que foi considerado que não existem medidas de preparação ou mitigação para este cenário, no entanto, isto pode não ser a realidade. Ainda assim, os ataques cibernéticos a infraestruturas críticas têm vindo a aumentar pelo que é um cenário a analisar detalhadamente.

Tabela 29 – Perfil de vulnerabilidade

C: Visão Geral da Vulnerabilidade

Vulnerabilidade muito elevada		Avaliação de Níveis de Vulnerabilidade		
Vulnerabilidade elevada		**Preparações (planos, medidas preventivas, etc.)**	**Capacidades de Resposta e Alívio**	**Capacidades de Recuperação**
Vulnerabilidade média				
Vulnerabilidade baixa				
Vulnerabilidade muito baixa				
Cenários de Ameaças	**Cenário 1 – Falha elétrica Silval**			
	Cenário 2 - Sismo			
	Cenário 3 – Avaria telegestão			Não se sabe
	Cenário 4 – Avaria bombas doseadores			
	Cenário 5 a) – Ataque cibernético			
	Cenário 5 b) – Destruição reservatório Silval			Não se sabe
	Cenário 5 c) – Contaminação da água			Não se sabe
	Cenário 6 – Falha do Carvoeiro			

A falha do Carvoeiro, Cenário 6, consiste num cenário com vulnerabilidade elevada. O Carvoeiro é o ponto de captação principal da rede e apesar da falha deste ser bastante improvável de ocorrer, é necessário ter em conta que o funcionamento desse ponto depende de uma empresa distinta da AdRA pelo que esta não tem a capacidade de garantir o funcionamento desse ponto.

A rede em estudo apresenta vulnerabilidade média ao cenário 3 pois consiste num evento que se espera que tenha curtas durações. Os reservatórios encontram-se vedados e fechados pelo que a contaminação ou destruição dos mesmos é dificultada resultando em probabilidades de ocorrência baixas. Assim, a vulnerabilidade da rede em estudo aos cenários 5 b) e 5 c) é também considerada média.

Os cenários para os quais se considera que a rede é menos vulnerável é a falha elétrica (cenário 1) e a avaria das bombas doseadoras (cenário 4), isto porque existe respetivamente um gerador e medidas de identificação e reparo da avaria que minimizam significativamente a vulnerabilidade da rede a esses cenários.

Por fim, em caso de ocorrência de sismo (cenário 2) não se conhecem as medidas de preparação existentes daí considerar-se uma alta vulnerabilidade no que respeita a preparação. Por outro lado, a ocorrência de sismos é uma temática que tem vindo a ser analisada e comunicada pelo que se considera que existem medidas de resposta, p.ex. por parte de entidades públicas como a Proteção Civil, e medidas de recuperação por parte da empresa, nomeadamente equipas de manutenção que reparam os danos.

3.5 Mapas de Risco

Na presente análise consideraram-se seis cenários de ameaças distintas, sendo que no caso da categoria de ameaça crime, foram desenvolvidos três cenários, cada um com um incidente distinto.

Como foi mencionado no ponto 3.3, o ponto Silval corresponde ao ponto mais crítico da rede, sendo que os cenários 1, 4, 5 b) e 5 c) consistem em ameaças a esse ponto. Os restantes cenários correspondem a ameaças às quais toda a rede está sujeita. Assim, foram elaborados dois mapas de risco que têm em conta as duas situações descritas. Os níveis de risco encontram-se na Tabela 30.

Tabela 30 - Níveis de Risco

	Risco muito elevado
	Risco elevado
	Risco médio
	Risco baixo
	Risco muito baixo
	Não relevante

A Figura 33 corresponde ao mapa de risco geral das ameaças ao ponto Silval, enquanto que na Figura 34 visualiza-se o mapa de risco geral das ameaças à rede. Estes mapas encontram-se no Anexo C.

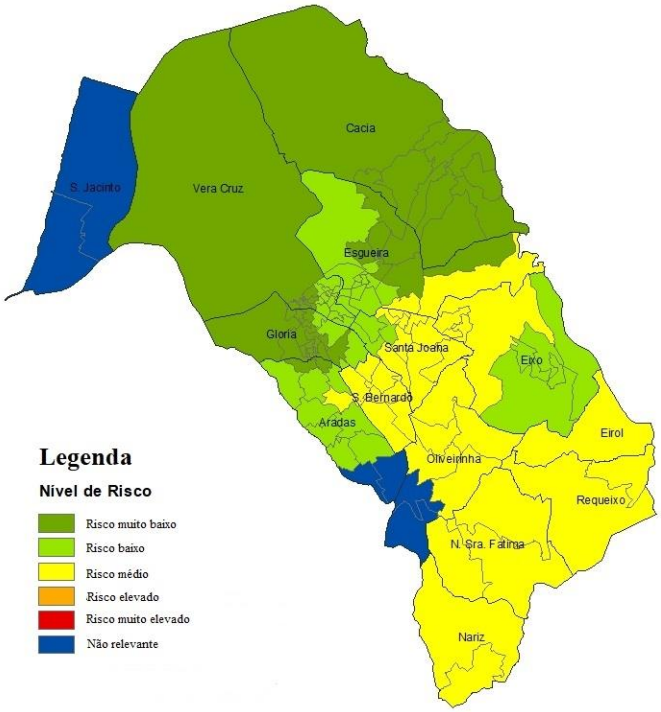


Figura 33 - Mapa de Risco – Cenários considerados nos reservatórios do Silval

Ao analisar o mapa de risco das ameaças ao ponto Silval verifica-se que os riscos são iguais ou inferiores a risco médio. Os cenários associados a este mapa são os cenários: 1 – falha elétrica, 4 – avaria de bombas doseadoras, 5 a) destruição do reservatório e b) contaminação de água.

As ameaças ao ponto Silval não afetam o ponto localizado em São Jacinto, visto que não existe ligação entre eles. No que respeita à restante rede, o ponto do Silval (ZA) tem um nível de risco mais elevado que os restantes visto que é afetado por todos os cenários considerados. O ponto Nariz encontra-se inativo sendo abastecido pelo Silval, logo tem o mesmo nível de risco. Tendo em conta que não se tem conhecimento das cotas de Nariz,

considerou-se que este corresponde a Zona Alta, pois é a situação mais desfavorável. O Silval (ZB) é menos afetado pelo cenário 1, justificando o nível de risco baixo. Os pontos Cacia e Cidade, apesar de estarem a ser abastecidos pelo Silval, têm capacidade para ser independentes do mesmo o que justifica o nível de risco muito baixo.

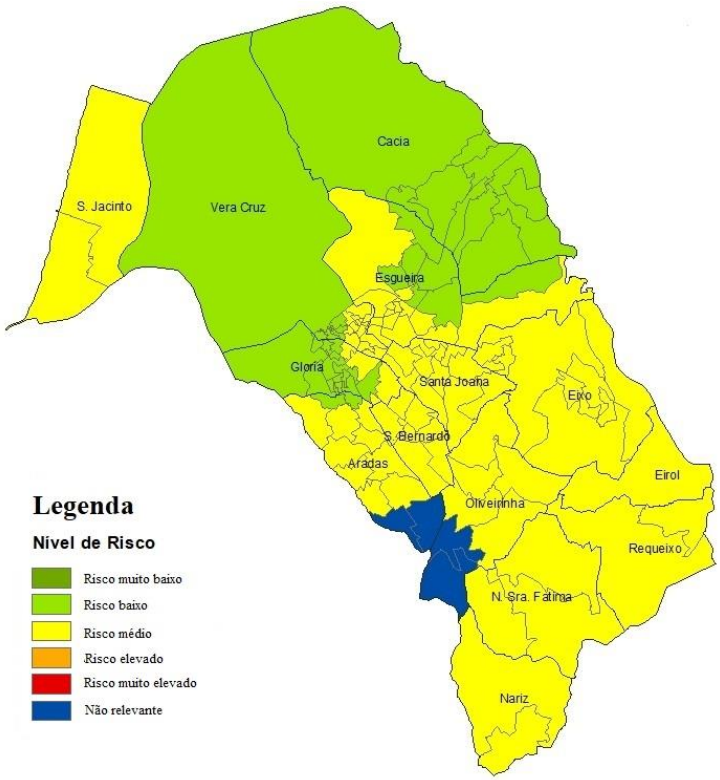


Figura 34 - Mapa de Risco - Ameaças à Rede

Analisando o mapa de risco ilustrado na Figura 34 é possível visualizar alterações no ponto São Jacinto e Silval (ZB). Tendo em conta que para cada cenário, a probabilidade de ocorrência é a mesma para todos os pontos da rede, no entanto as consequências são distintas para cada ponto. Os pontos com nível médio correspondem aos pontos que não têm subsistemas, resultando em consequências mais severas.

3.6 Planos a desenvolver

A gestão de risco tem como objetivo minimizar os impactos de potenciais riscos a que uma certa atividade esteja sujeita, através do melhor entendimento dessa atividade. No caso de infraestruturas, analisar o seu comportamento quando sujeita a determinados eventos, associados a potenciais riscos, permite identificar que medidas se devem implementar, de forma a minimizar as consequências do evento.

Neste ponto são identificadas algumas medidas e planos que devem ser desenvolvidos para diminuir a vulnerabilidade da rede em estudo.

No Anexo E encontram-se um exemplo para cada um dos planos, de contingência e emergência.

1. **Planos de Manutenção;**
2. **Planos de Investimento;**
3. **Plano de Contingência:** visa preparar a organização a responder eficazmente a emergências e seu potencial impacto humanitário.
4. **Planos de Emergência:** sistematização de um conjunto de normas e regras de procedimentos destinadas a minimizar os efeitos das catástrofes que se prevê que possam vir a ocorrer, gerindo, de uma forma otimizada, os recursos disponíveis (Ferreira, 2007);
   - **4.1. Plano de Evacuação;**
   - **4.2. Plano de Ação;**

Capítulo 4

Considerações Finais

Capítulo 4 – Considerações Finais

4.1 Síntese do trabalho realizado

4.2 Conclusões e trabalhos futuros

4 Considerações Finais

4.1 Síntese do trabalho realizado

A consciencialização da importância das infraestruturas críticas para o dia-a-dia da sociedade é um trabalho a realizar. Atualmente, as ameaças às infraestruturas críticas aumentam regularmente pelo que deve ser tomada uma atitude ativa, de forma a garantir a segurança da sociedade. Essas ameaças, não correspondem apenas a atos intencionais humanos, como criminalidade ou terrorismo, mas também a fenómenos naturais que têm vindo a ocorrer nos últimos anos devido ao aquecimento global, e sobre os quais não se tem qualquer controlo.

O presente trabalho pretende contribuir para que as empresas responsáveis por infraestruturas críticas realizem a gestão de risco dos seus ativos, de forma a garantir o adequado funcionamento das mesmas, em particular, em situações de concretização dos riscos que lhes estão associados.

O estudo desenvolvido foi aplicado ao caso de estudo rede de abastecimento de água de Aveiro, constituída por 15 reservatórios, 5 elevados e 10 apoiados, localizados em 5 freguesias distintas. A rede abastece aproximadamente 78450 pessoas, população do concelho de Aveiro de acordo com os CENSOS 2011.

O caso de estudo foi analisado através da utilização do *ArcMap* do *software ArcGis desktop*. Com essa ferramenta foi analisado o funcionamento da rede e a população que depende do abastecimento, sendo assim possível identificar os pontos críticos da rede.

Nesta dissertação foi realizada a avaliação de risco do caso de estudo a partir da metodologia desenvolvida na Dinamarca, *Risk and Vulnerability Analysis*, RVA. Esta metodologia consiste no preenchimento de quatro *templates* disponibilizados no site da *Danish Emergency Management Agency*, DEMA. No primeiro identificam-se os intervenientes na análise e as funções críticas da sociedade a analisar. O segundo e o terceiro correspondem, respetivamente à identificação das ameaças e à análise dos cenários de ameaças, por fim, no quarto *template* elabora-se o perfil de risco e estima-se a vulnerabilidade. Desenvolveram-se 8 cenários associados a seis categorias de ameaças distintas.

A avaliação de risco à rede permitiu verificar os cenários com riscos mais elevados e identificar vulnerabilidades da rede. Após o preenchimento dos *templates*, para cada um dos cenários, desenvolveu-se uma análise geral e identificaram-se possíveis medidas a implementar de forma a melhor a preparação ou resposta da empresa ao incidente.

Relativamente aos perfis de risco e vulnerabilidade, a matriz de risco permite verificar que os cenários desenvolvidos têm níveis de risco baixo ou médio, sendo que as probabilidades e os níveis de risco não são os mesmos para todos os cenários. A matriz facilita ainda a identificação dos cenários com maior probabilidade de ocorrência e os cenários que resultam em consequências mais graves. Isto permite escolher os cenários para os quais o investimento em medidas de preparação e mitigação deve ser prioritário (hierarquização de medidas a implementar).

Desenvolveram-se ainda mapas de risco relativamente aos cenários que afetam a rede em geral e aqueles que afetam o seu ponto mais crítico, o Silval. Por fim, identificaram-se alguns planos a desenvolver de forma a garantir preparação e capacidades de reposta e recuperação adequadas em caso de ocorrência de eventos adversos. Ainda relativo aos planos a desenvolver foram integrados em anexo exemplos para a estrutura desses planos.

4.2 Conclusões e trabalhos futuros

O trabalho realizado ao longo desta dissertação teve como objetivo analisar o comportamento da rede de abastecimento do concelho de Aveiro em caso de ocorrência de potenciais riscos, identificando as ameaças a que a rede está sujeita e analisar as vulnerabilidades da mesma.

Após o desenvolvimento da análise da rede conclui-se que a rede se encontra preparado para riscos técnicos como a falha elétrica e a avaria de bombas doseadoras, no entanto no que respeita a catástrofes naturais ou intenções criminosas identificaram-se algumas vulnerabilidades da rede, nomeadamente a ataques cibernéticos ou a falha do Carvoeiro.

Durante a análise da rede considerou-se em alguns casos que não existem medidas de preparação ou planeamento. Assim, sugere-se que, para esses casos, as análises sejam complementadas com a informação adequada, de forma a melhorar a análise desenvolvida.

O contributo do estudo desenvolvido na presente dissertação poderá ser ampliado em futuros trabalhos de investigação na área da gestão de risco de infraestruturas críticas. A temática da gestão de riscos tem vindo a tornar-se cada vez mais importante devido ao aumento de ameaças às infraestruturas críticas e das consequências das mesmas.

Sugere-se para trabalhos futuros o desenvolvimento de *software* que realize a gestão de risco de infraestruturas críticas de forma mais rápida, completa e eficiente. Apesar de já existirem softwares com essas funções, consistem principalmente em ferramentas governamentais que não se encontram disponíveis.

Os *softwares* a desenvolver devem ter em consideração o tipo de infraestrutura sendo que cada infraestrutura crítica tem funções e objetivos diferentes. Esse *software* deve aplicar avaliações de risco abrangentes que considerem interdependências entre infraestruturas de um sistema e entre sistemas.

Os *softwares* podem revelar-se ferramentas muito úteis para empresas que gerem infraestruturas críticas, sendo recomendada a colaboração entre essas empresas e universidades, com o intuito de melhorar a gestão das infraestruturas críticas. Aconselha-se a que *software* seja uma ferramenta intuitiva que apesar de realizar análises complexas, permita a sua utilização a técnicos não especializados.

Referências Bibliográficas

Referências Bibliográficas

Albert, R. Barabasi, A. L. 2002. *Statistical mechanics of complex networks*, Reviews of Modern Physics, vol. 74, no. 1, pp. 47-97, 2002

AdRA 2017. Empresa – Quem Somos [Online]. Aveiro: AdRA Disponível em: http://www.AdRA.pt/content/index.php?action=detailfo&rec=1800&t=Quem-somos. [Acedido a 12 de junho de 2017]

APFM 2017. Sobre a APFM [Online]. Lisboa: Associação Portuguesa de *Facility Management*. Disponível em: http://apfm.pt/sobre-a-apfm/. [Acedido a 12 de junho de 2017]

APSEI 2017. Gestão de risco [Online]. Sacavém: Associação Portuguesa de Segurança. Disponível em: https://www.apsei.org.pt/areas-de-atuacao/protecao-civil/protecao-e-gestao-de-risco-de-infraestruturas-criticas/. [Acedido a: 8 de junho de 2017]

Assad, E. Sano, E. 1998. Sistemas de Informação Geográfica – Aplicações na Agricultura, 2ª Edição, Brasília, Embrapa – CPAC.

Baker, G. H. Redwine, S. Blandino, J. 2003. *Network Security Risk Assessment Modelling Tools for Critical Infrastructure Assessment, College of Integrated Science and Technology, James Madison University*.

Barton, D. C. Edison, E. D. Schoenwald, D. A. Cox, R. G. Reinert, R. K. 2004. *Simulating Economic Effects of Disruptions in the Telecommunications Infrastructure, Sandia National Laboratories*.

http://www.jmu.edu/iiia/wm_library/Network_Security_Risk_Assessment_Modeling_(NSRAM).pdf

Brashear, J. P. Jones, J. W. 2009, *All-Hazards Risk and Resilience, Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach* [Online], Nova Iorque: ASME. Disponível em: http://files.asme.org/ASMEITI/RAMCAP/17978.pdf. [Acedido a: 15 de janeiro de 2017]

Bush, B. B. Dauelsberg, L. R. LeClaire, R. J. Powell, D. R. DeLand, S. M. Samsa, M. E. 2005. *Critical Infrastructure Protection Decision Support System (CIP/DSS) – Project Overview, International Systems Dynamics Conference*.

Caldwell, Stephen L. 2009. *Department of Homeland Security's Critical Infrastructure Protection Cost-Benefit Report*, page 2.

Censos 2011. Densidade Populacional [Online], Lisboa: Instituto Nacional de Estatística. Disponível em: http://mapas.ine.pt/map.phtml [Acedido a: 5 de Novembro de 2017]

Chang, K. 2007. *Geographic Information System* [Online], *The International Encyclopaedia of Geography*. Disponível em:

http://onlinelibrary.wiley.com/doi/10.1002/9781118786352.wbieg0152/abstract;jsessionid=AF6C1BE20AFB7E1D304C290D656A8B74.f01t02?userIsAuthenticated=false&deniedAccessCustomisedMessage [Acedido a: 24 de junho de 2017]

Deane, M. 2003. *Water Utility Sector Works in Partnership to Meet Cyber Security Challenges* [Online]. The Huffington Post – Business. Disponível em: http://www.huffingtonpost.com/michael-deane/water-utility-sector-work_b_4373213.html. [Acedido a: 16 de junho de 2017]

DHS 2017. *National Infrastructure Protection Plan – Risk Management Framework* [Online]. Washington DC: Department of Homeland Security, DHS. Disponível em: https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf [Acedido a: 6 de dezembro 2017]

DA 1991. *Special Operations Forces Intelligence and Electronic Warfare Operations*, Field Manual, Anexo D. Washington DC, *Department of the Army*.

DEMA 2006. *RVA model: Introduction and User Guide – DEMA´s model for risk and Vulnerability Analysis* [Online]. *Birkeød: Danish Emergency Management Agency*. Disponível em: http://brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx. [Acedido a: 12 de janeiro de 2017]

Eidson, E. D. Ehlen, M. A. 2003. *NISAC Agent-Based Laboratory for Economics (N-ABLE): Overview of agent and simulation architectures*. Novo México: Sandia National Laboratory.

Espelund, G. 2016. *How vulnerable are water utilities to traditional and cyber threats?* [Online] Aurora, Canadá: *Environmental, Science & Engineering*. Disponível em:

https://esemag.com/featured/how-vulnerable-are-water-utilities-to-cyber-threats/ [Acedido a: 5 de junho de 2017]

ESRI 1998. ESRI *Shapefile Technical Description*, Redlands, Califórnia, ESRI.

ESRI 2017. *About ArcGIS* [Online]. Redlands: ESRI. Disponível em: http://www.esri.com/arcgis/about-arcgis [Acedido a: 24 de junho de 2017]

Ferreira, I. 2007. O Plano de Emergência: A sua importância. Monografia apresentada para a obtenção de licenciatura em Gestão de Empresas, Universidade Fernando Pessoa, Porto.

FMA 2004. *Facility Management Guidelines to Managing Risk* [Online], Melbourne: Facility Management Association Australia. Disponível em: https://www.academia.edu/10239744/Facility_Management_Guidelines_to_Managing_Risk. [Acedido a 12 de junho de 2017]

Gallaher, M., O'Connor, A., Dettbarn, Jr. J., and Gilday, L. 2004. *Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry,* Maryland, *National Institute of Standards and Technology.*

GSA , 2012. *Facility Management* [Online], Washington, DC: *US General Services Administration*. Disponível em: https://www.gsa.gov/portal/content/122555 [Acedido a 3 de Dezembro de 2016]

Giannopoulos, G. Filippini, R. Schimmer, M. 2012. *Risk assessment methodologies for critical infrastructure protection: Part I: A state of the art, European Commission – Joint Researched Centre, Institute for the Protection and Security of the Citizen. (fonte original não disponível)*

Grimm, V. Railsback, S. F. 2005. *Individual-based modelling and Ecology* [e-book], Princeton: Princeton University Press. Disponível em: http://press.princeton.edu/titles/8108.html [Acedido a: 15 de janeiro de 2017]

Goodwin, B. L. Lee, L. 2005. *Planning and Assessing Effects Based Operations, International Command and Control Research and Technology Symposium the Future of Command and Control, SPARTA.*

Haimes, Y. Y. 2006. *On the Definition of Vulnerabilities in Measuring Risks to Infrastructures, Risk Analysis – A International Journal,* volume 26, edição 2.

DHS 2017. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* [Online], Washington DC: Departamento de Segurança Interna. Disponível em: https://www.dhs.gov/homeland-security-presidential-directive-7 [Acedido a: 08 de janeiro 2017]

IFMA 2017. *What is Facility Management* [Online], Houston: *International Facility Management Association*. Disponível em: https://www.ifma.org/about/what-is-facility-management [Acedido a: 11 de Janeiro de 2017]

IPMA 2017. Escala de Mercalli Modificada, 1956 [Online]. Lisboa: Instituto Português do Mar e da Atmosfera. Disponível em: http://www.ipma.pt/pt/enciclopedia/geofisica/escalas.macro/index.html. [Acedido a: 04 de junho de 2017]

Jaeger, C. D. Roehrig, N. S. Torres, T. 2008. *Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures (Report), Sandia National Laboratories*.

Kelic, A. Warren, D. E. Phillips, L. R. 2008. *Cyber and Physical Infrastructure Interdependencies* (Report), *Sandia National Laboratories*.

Kumpulainen, S. 2006. *Vulnerability concepts in hazard and risk assessment. Natural and technological hazards and risks affecting the spatial development of European regions, Geological Survey of Finland,* Special Paper 42, 65–74.

LNEC 2017. Informações de Interesse Geral: O que são sismos? [Online], Lisboa: Departamento de Estruturas, Núcleo de Engenharia Sísmica e Dinâmica de Estruturas, Laboratório Nacional de Engenharia Civil. Disponível em: http://www-ext.lnec.pt/LNEC/DE/NESDE/divulgacao/o_que_sao_sismos.html. [Acedido a: 13 de maio de 2017]

Multi-Hazard Mitigation Council, MMC (2005), *Mitigation Saves: The Benefits of FEMA Hazard Mitigation Grants, National Institute of Building Sciences*.

NISAC *2017. Capabilities Fact Sheets, FASTMap,* Washington, DC: DHS. Disponível em: http://www.sandia.gov/nisac/wp/wp-content/uploads/FASTMap-20160411-SAND2016-3381M.pdf. [Acedido a: 11 de abril de 2017]

Oliveira, 2015. A segurança de infraestruturas críticas em Portugal. Dissertação apresentada para a obtenção do grau de Mestre em Direito e Segurança, Faculdade de Direito da Universidade Nova de Lisboa, Lisboa.

Ostfeld, A. 2006. *Enhancing Water-Distribution System Security through Modelling, Journal of Water Resources Planning and Management*, volume 132.

PCM 2008. Plano de Emergência Interno do Lar, Câmara Municipal de Mafra.

PCL 2017. Conhecer para Prevenir: O Risco Sísmico na Cidade de Lisboa [Online], Lisboa: Proteção Civil de Lisboa. Disponível em: http://idl.campus.ciencias.ulisboa.pt/wp-content/uploads/2016/12/sismos.pdf. [Acedido a: 04 de junho de 2017]

PSC 2009. *National Strategy for Critical Infrastructure, NSCI* [Online] Canadá: Public Safety Canada. Disponível em: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx. [Acedido a: 21 de janeiro 2017]

Petit, F. D. Basset, G. W. Buehring, W. A. Collins, M. J. Dickinson, D. C. Haffenden, R. A. Huttenga, A. A. Klett, M.S. Phillips, J. A. Veselka, S. N. Wallace, K. E. Whitfield, R. G. Peerenbcom, J. P. 2013. *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, Decision and Information Sciences Division, Argonne National Laboratory.

Pye, G. Warren, M. 2006. *Critical Infrastructure Protection, Modelling and Management: An Australian Commercial Case Study*, School of Information Systems, Deakin University.

Rodrigues, 2013. A gestão de risco – estudo da sua influência na competitividade dos municípios portugueses. Dissertação apresentada para a obtenção do grau de Mestre em Controlo de Gestão, Escola Superior de Tecnologia e Gestão, Leiria.

Roozbahani, A. Zahraie, B. Tabesh, M. 2012. *Integrated risk assessment of urban water supply systems from source to tap,* Springer, Volume 27, p. 923–944

Rose, A. 2006. *Economic Resilience to Disasters: Toward a Consistent and Comprehensive Formulation, Disaster Resilience: An Integrated Approach, Springfield, IL*: Charles C. Thomas, 2006, pp. 226-48

Saleh, A., Kamarulzaman, N., Hashim, H., Hashim S. 2011. *An Approach to Facilities Management (FM) Practices in Higher Learning Institutions to Attain a Sustainable Campus (Case Study: University Technology Mara -UiTM), The 2nd International Building Control Conference.*

Samsa, M. E. VanKuiken, J. C. Jusko, M. J. 2008. *Critical Infrastructure Protection Decision Support System – Decision Model: Overview and Quick-Start User's Guide*, Argonne National Laboratory.

SFP 2011. *European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks* [Online], Hialeah: Seventh Framework Programme. Disponível em: https://pt.scribd.com/document/259385488/Euracom-Risk-Assessment-and-Contingency-Planning-Methodologies. [Acedido a: 20 de janeiro de 2017]

Silva, J. 2013. Princípios para o desenvolvimento de projetos com recurso a ferramentas BIM. Dissertação apresentada para a obtenção do grau de Mestre em Engenharia Civil, Faculdade de Engenharia da Universidade do Porto, Porto.

Sirohi, Dr. M. N. 2016. *Understanding Network Centric Warfare* [e-book], New Deli: Alpha Editions. Disponível em: https://books.google.pt/books?isbn=9385505734 [Acedido a 04 de Março de 2017]

Sousa, E. 2003. Telegestão em Sistema de Abastecimento de Água, Secção de Hidráulica e de Recursos Hídricos e Ambientais, Departamento de Engenharia Civil e Arquitetura, Instituto Superior Técnico, Lisboa.

Stamber, K. L. Brown, T. J. Pless, D. J. Berscheid, A. 2013. *Modelling and Simulation for Homeland Security, 20th International Congress on Modelling and Simulation*.

Tularam, A. G. Properjohn, M. 2011. *An investigation into modern water distribution network security: Risk and implications*, Security Journal, Volume 24, p 283–301.

Utne, I. B. Hokstad, P. Kjolle, G. Vatn, J. Tondel, I. A. Bertelsen, D. Fridheim, H. Rostum, J. (2012) *Risk and Vulnerability Analysis of Critical Infrastructure – The DECRIS Approach*, Risk and Interdependencies in Critical Infrastructures, p 23-33.

UNDP 2010. *Urban Risk Assessment* [Online], Nova Iorque: *United Nations Development Programme.* Disponível em: http://www.undp.org/content/dam/undp/library/crisis%20prevention/disaster/2Disaster%20Risk%20Reduction%20-%20Risk%20Assessment.pdf. [Acedido a 5 de outubro de 2016]

Vasyl, Z. Mikulas, L. Republik, S. 2013. *Danger - a subjective evaluation of objective reality,* Science & Militar e Armed Forces Academy of General Milan Rastislav Stefanik. No 1, Volume 8, P. 53-62

Vesely, W. E. Goldberg, F. F. Roberts, D. H. Haasl, D. F. 1981. *Fault Tree Handbook, US Nuclear Regulatory Commission.*

Vieira, J. Valente, J. Peixoto, F. Morais, C. 2006. Elaboração e Implementação de Planos de Contingência em Sistemas de Abastecimento de Água, 8º Congresso da Água, Figueira da Foz.

Anexos

Anexo A – Tabela resumo – Metodologias

Anexo B- Esquema da Rede de Abastecimento (AdRA)

Anexo C - Mapas da Rede de Abastecimento (*ArcMap)*

Anexo D - *Templates* preenchidos

Anexo E - Exemplos planos a desenvolver

Anexo A – Tabela resumo – Metodologias

Nome	Objetivos	Sectores/Perigos	Interdep.	Resiliência	Vantagens	Desvantagens
1. BIRR	Avaliação de riscos e resiliência de infraestruturas	18 setores/Catástrofes Naturais e Perigos de Origem Humana	Sim	Sim	Considera resiliência; Quantificação dos índices PMI, VI, RMI e CMI.	Coleta de informação através de ferramenta IST (software)
2. PIC/DCP	Identificação de ameaças, riscos, vulnerabilidades e medidas de proteção. Incentivar a cooperação entre operadores de infraestruturas críticas e o governo	Todos os sectores/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	Interdependências como efeitos secundários;	Não foi encontrada bibliografia relativa à metodologia, exceto o artigo (Giannopoulos *et al., 2012)*
3. CARVER2	Avaliação de riscos e vulnerabilidade	Todos os sectores/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Sim (parc.)	Considera critérios importantes como a vulnerabilidade, interdependências e resiliência.	Software
4. CIMS	Tomada de decisões rápida. Priorização de operações de emergência	Todos os sectores/Catástrofes Naturais e Perigos de Origem Humana	Sim	Sim (impl.)	Construção de modelos através de mapas simples ou imagens aéreas, que permite a sua atualização em tempo real, com base na informação disponível do evento.	Não foi encontrada bibliografia relativa à metodologia, exceto o artigo (Giannopoulos *et al., 2012)*
5. CIP/DSS	Avaliação de riscos, consequências e vulnerabilidades	18 setores (2.3.2)/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	Determinação de uma estimativa do impacto do evento; Caracterização dos decisores;	Software

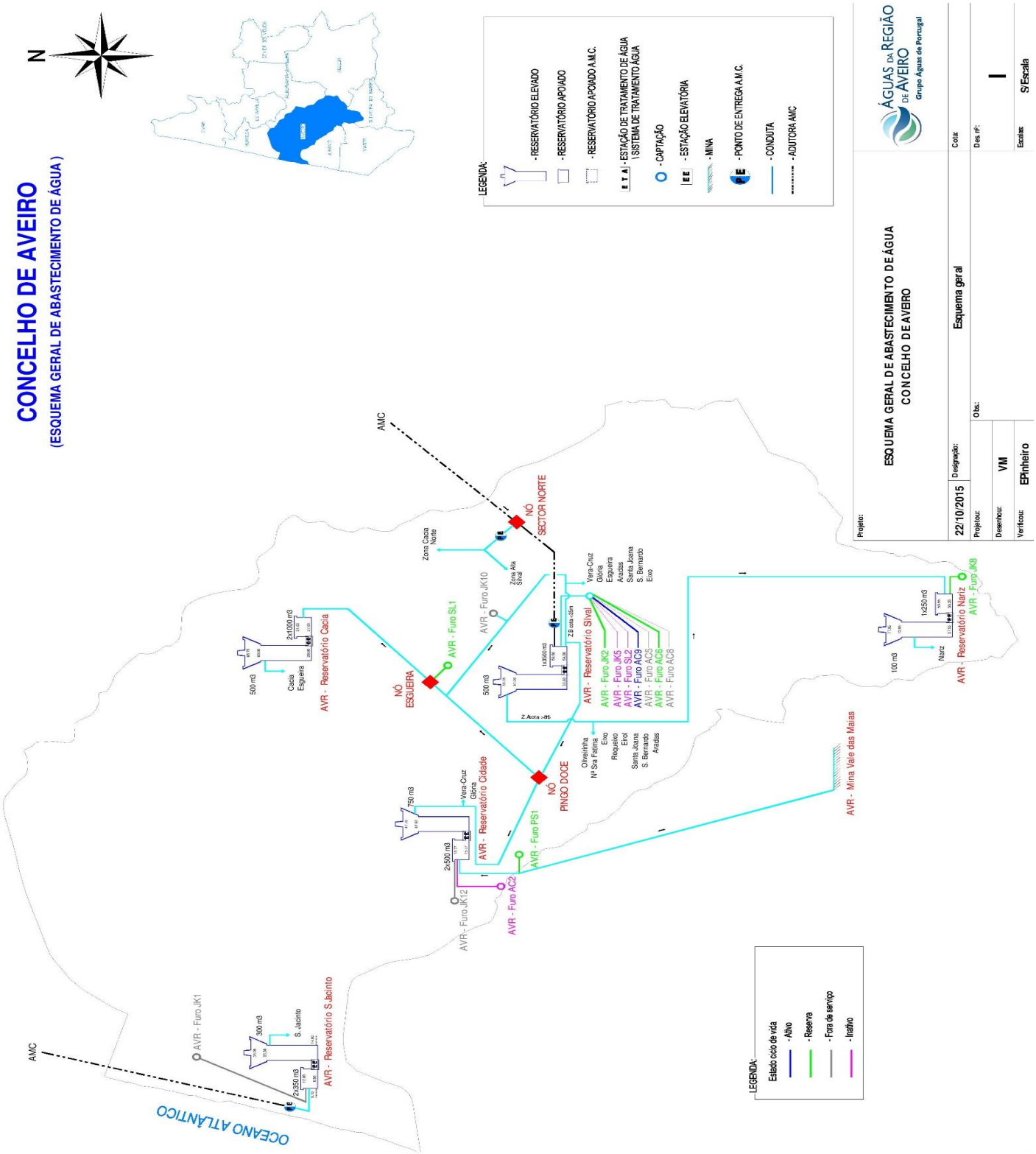
6. CIPMA	Avaliação de riscos, consequências e vulnerabilidades. Identificação de estratégias de mitigação e investimento	Sectores bancário, financeiro, energia e telecomunicações/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Sim (parc.)	Resiliência parcialmente considerada; Desenvolvimento de mapas de risco.	Software; Apenas aplicado a determinados sectores.
7. CommAspen	Avaliação do impacto em caso de interrupção de infraestruturas críticas	Sectores energia elétrica, finanças e telecomunicações/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	Modelação *agent-based*;	Software; Apenas aplicado a determinados sectores.
8. DECRIS	Avaliação de riscos e vulnerabilidades. Priorização de cenários	Sectores energia elétrica, abastecimento de água, transportes e sist. de informação e comunicação/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	Passos de aplicação da metodologia conhecidos;	Não é considerada a resiliência.
9. EURACOM	Avaliação de risco holística entre sectores. Tornar infraestruturas do setor da energia mais resilientes	Sectores energia/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	Abordagem holística;	Não é considerada a resiliência.
10. Anál. Rápida	Avaliação de vulnerabilidades e impacto da interrupção	Todos os sectores/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	Metodologia enfatiza as interdependências; Ferramentas REAcct e FAST*map*	Software; Não é considerada a resiliência.
11. MIN	Generalizar o paradigma das redes de transportes para outras infraestruturas e instituir a otimização	Sector dos transportes/Perigos técnicos	Sim	Não	Modelação agent-based;	Não foi encontrada bibliografia relativa à metodologia, exceto o artigo (Giannopoulos et al., 2012)
12. N-ABLE	Identificação dos sectores económicos mais vulneráveis à interrupção de infraestruturas críticas	Todos os sectores/Perigos técnicos e económicos	Sim	Não	Modelação agent-based;	Software

13. NEMO	Avaliação de operações em tempo real	Todos os sectores/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Sim (impl.)	Relações *on/off;* Mapeamento em GIS;	Software
14. NSRAM	Determinar interação e resposta dos sistemas a eventos adversos	Todos os sectores/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Sim	Modelação *agent-based*; Modela o comportamento humano;	Software
15. RAMCAP-*plus*	Identificação, priorização e coordenação da preparação de infraestruturas críticas	Todos os sectores/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Sim	A resiliência é o elemento central da metodologia; Permite a quantificação da resiliência.	Software
16. RVA	Avaliação de ameaças, riscos e vulnerabilidades	Todos os sectores/ Catástrofes Naturais e Perigos de Origem Humana	Não (expl.)	Sim	Ferramentas para aplicação disponíveis;	Não são consideradas as interdependências.
17. SRAM	Avaliação de risco e vulnerabilidade	Todos os sectores/ Terrorismo	Não abordada expli.	Não	Passos de aplicação da metodologia conhecidos; Determinação de risco condicional que permite a comparação entre infraestruturas da mesma instituição.	Software
18. NIPP	Avaliação de riscos, consequências e vulnerabilidades. Identificação de estratégias de mitigação	18 setores /Catástrofes Naturais e Perigos de Origem Humana	Não	Não	-	Não é considerada a resiliência.
19. GRSIC	Promover a colaboração de forma a melhorar a resiliência das infraestruturas	10 setores/Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	Consideração de interdependências em duas fases;	Não foi encontrada bibliografia relativa à metodologia, exceto o artigo (Giannopoulos et al., 2012)
20. GRAPS	Identificação, análise e apreciação de risco	Sectores da energia e transportes/ Catástrofes Naturais e Perigos de Origem Humana	Sim	Não	-	Não é considerada a resiliência.

Anexo B- Esquema da Rede de Abastecimento (AdRA)

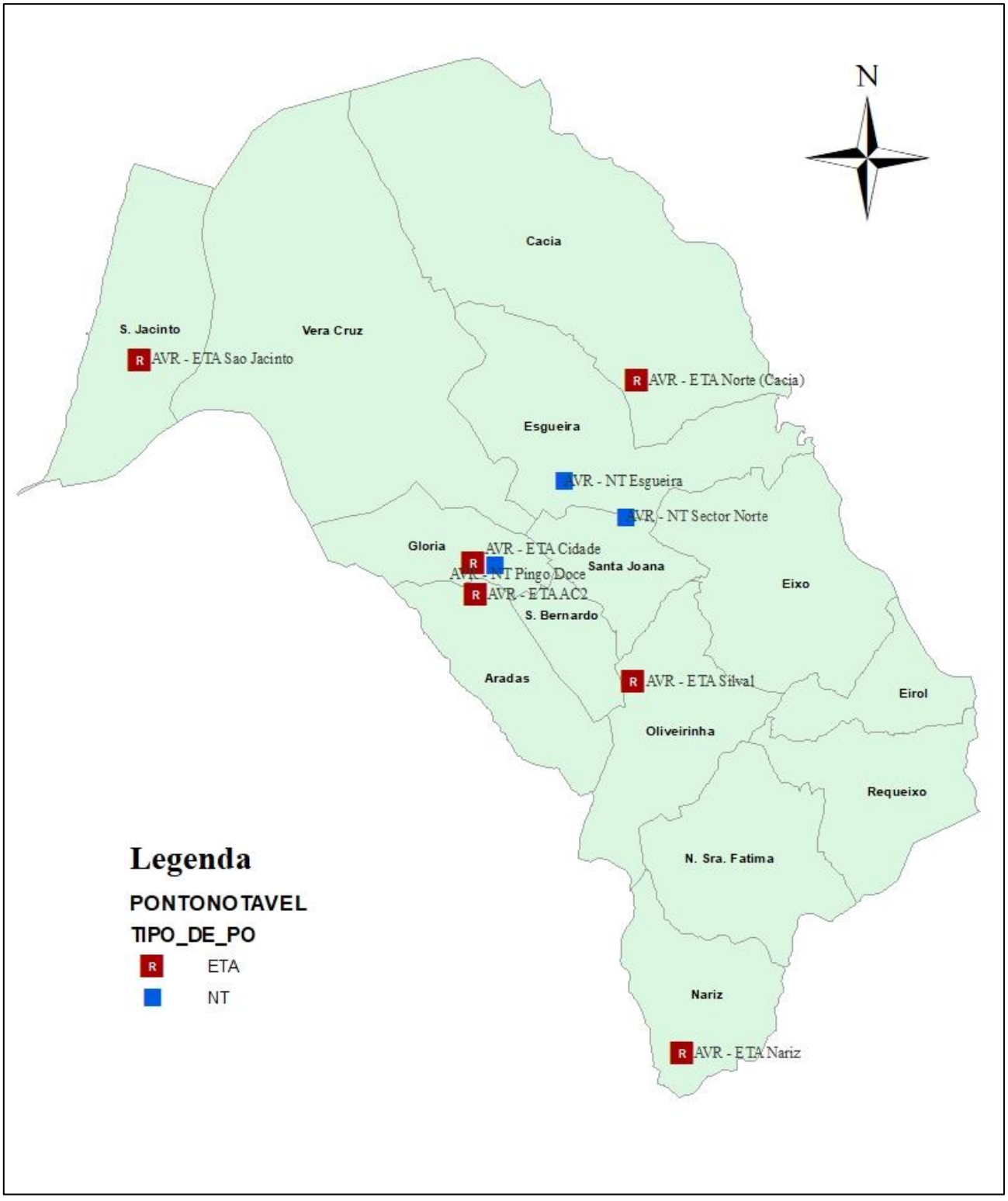
Esquema Geral de Abastecimento de Água

Concelho de Aveiro

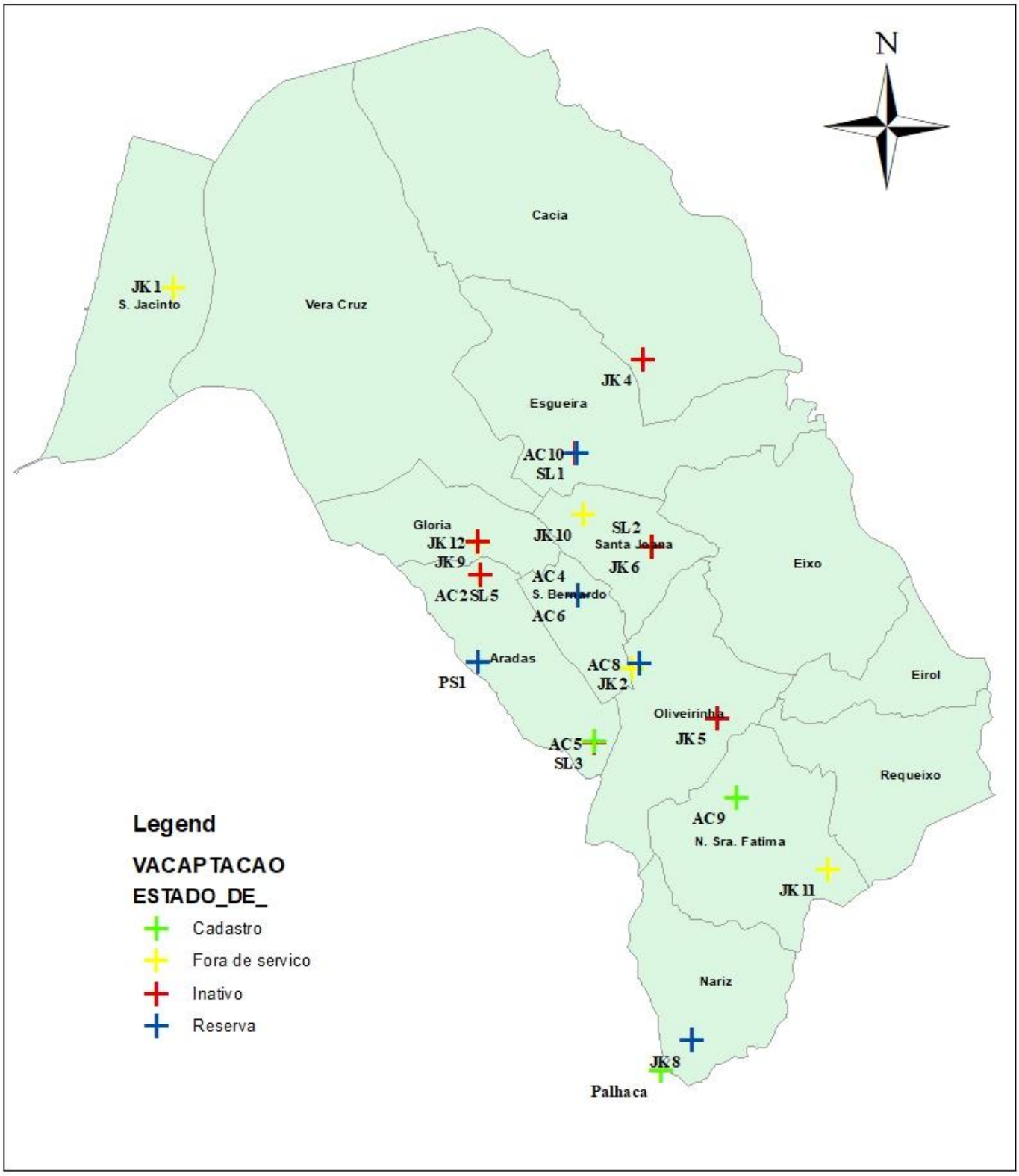


Anexo C - Mapas da Rede de Abastecimento (*ArcMap)*

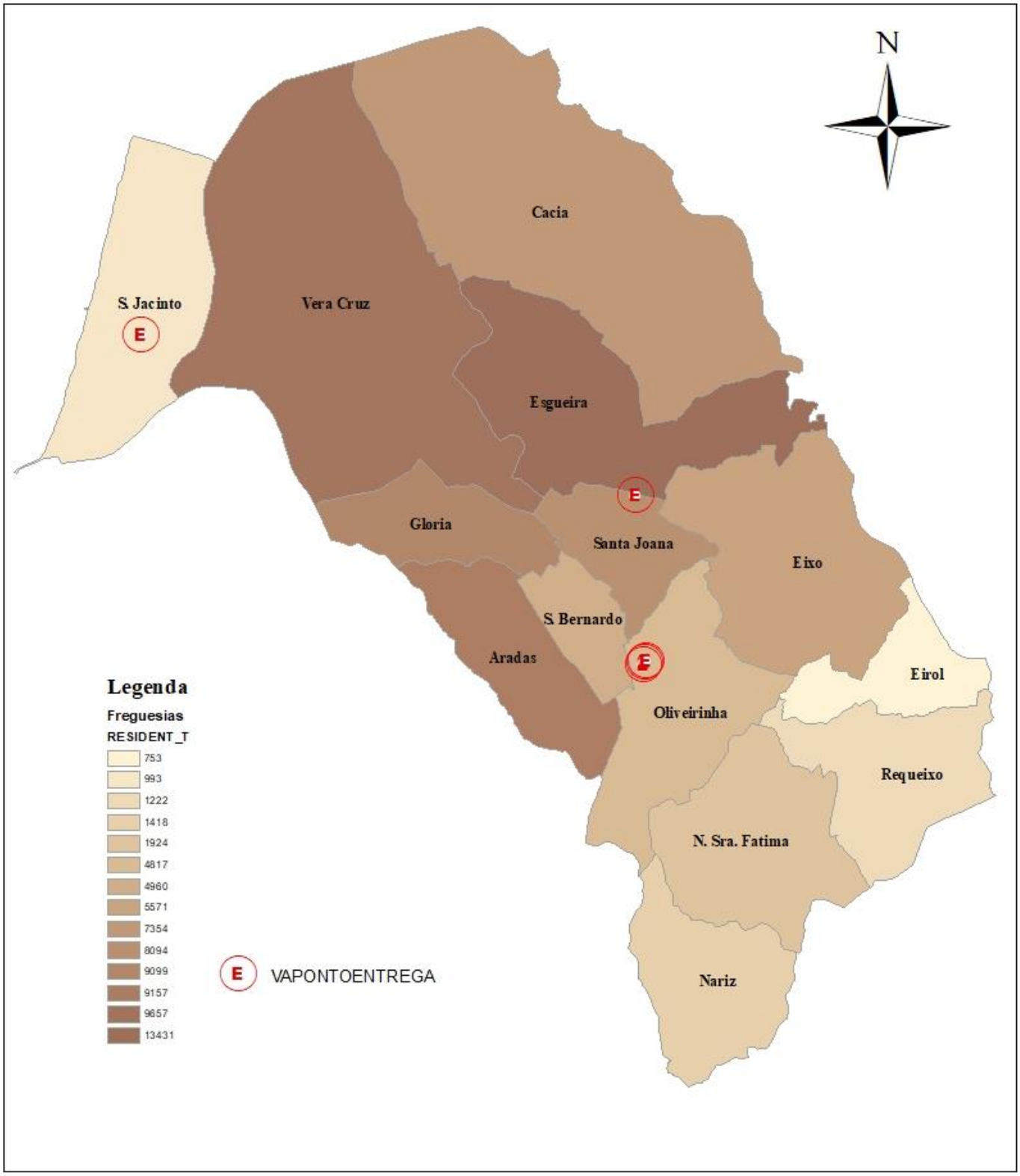
Mapa 1 – Pontos Notáveis



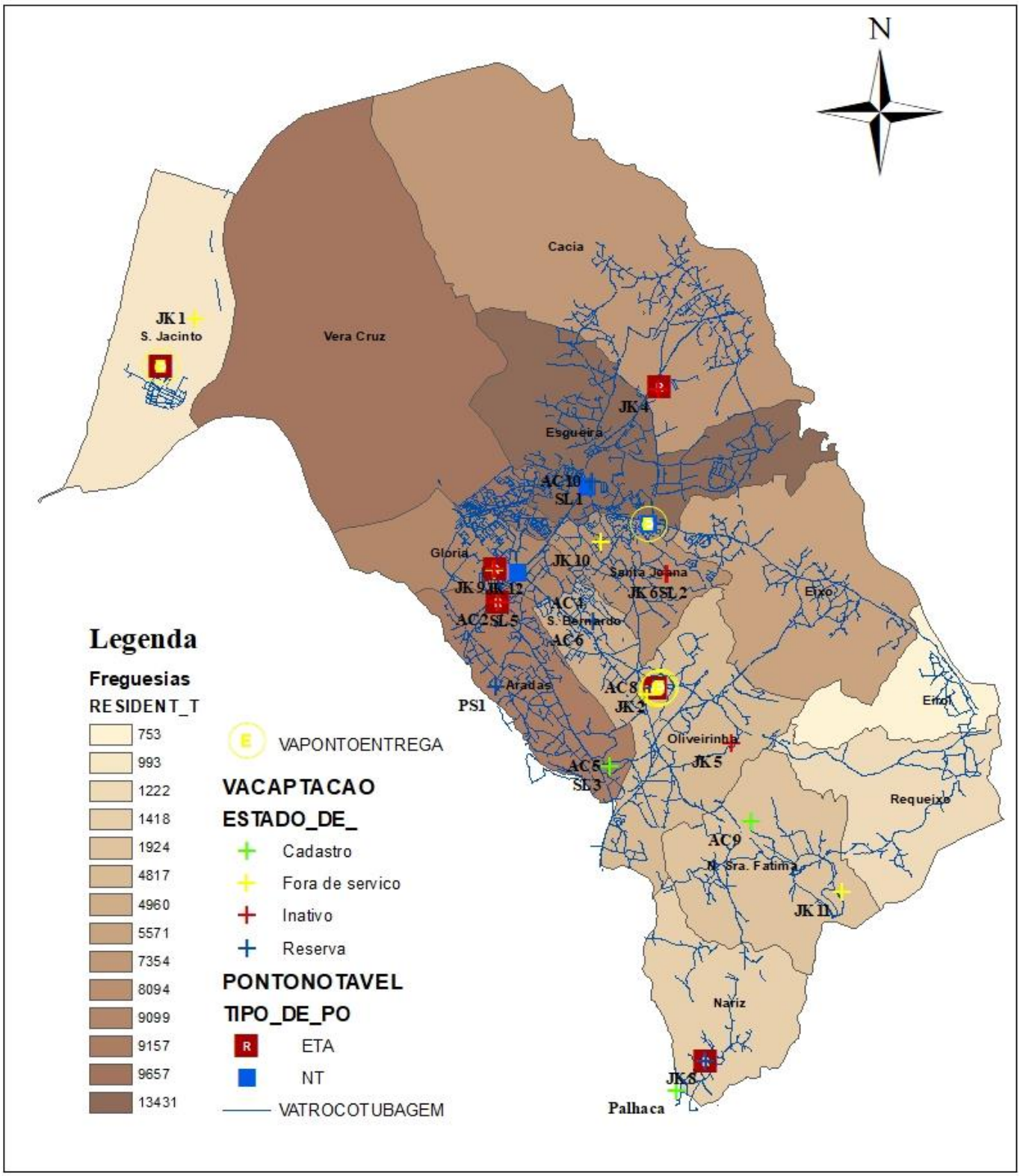
Mapa 2 – Pontos de Captação



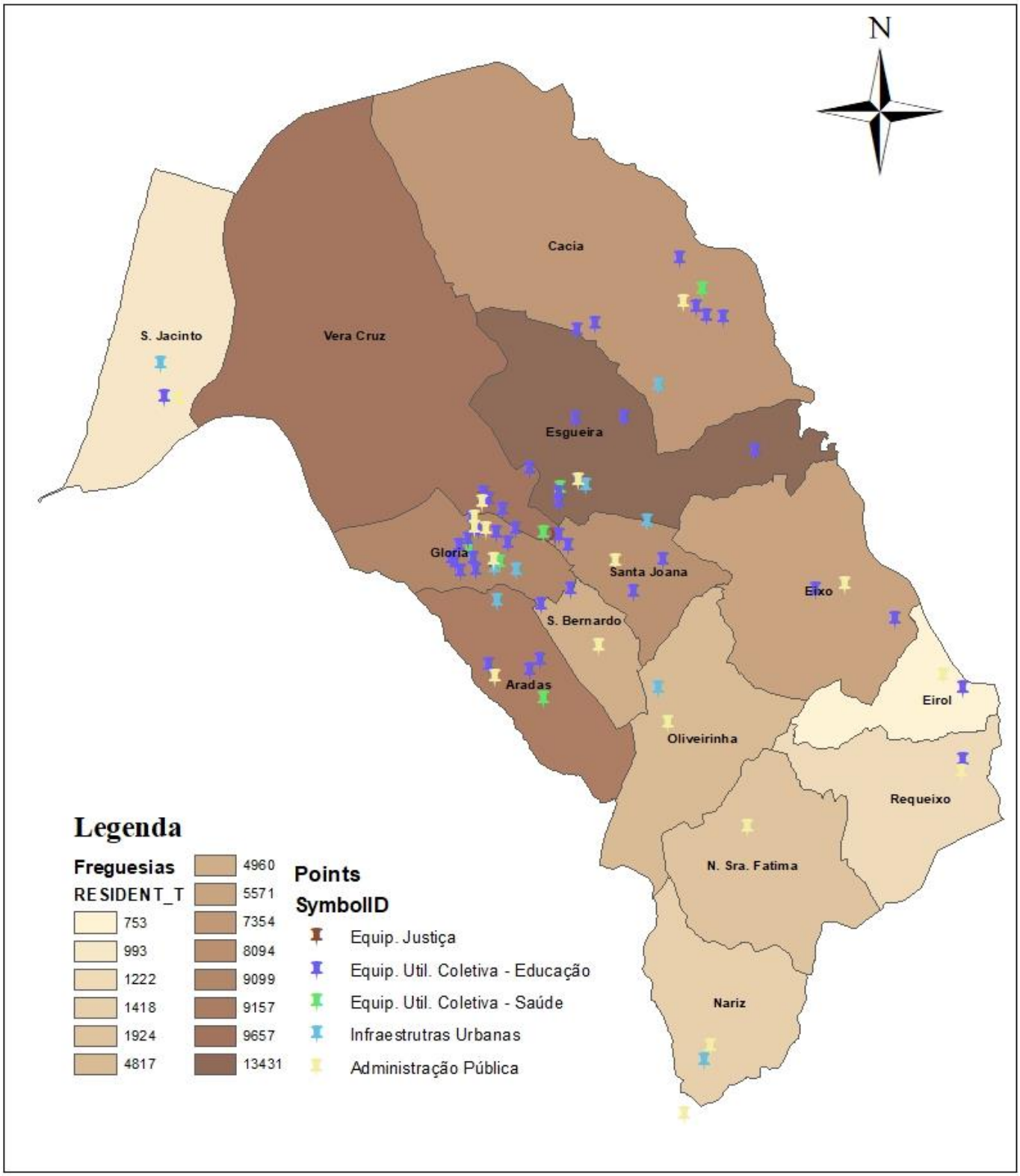
Mapa 3 – Pontos de Entrega



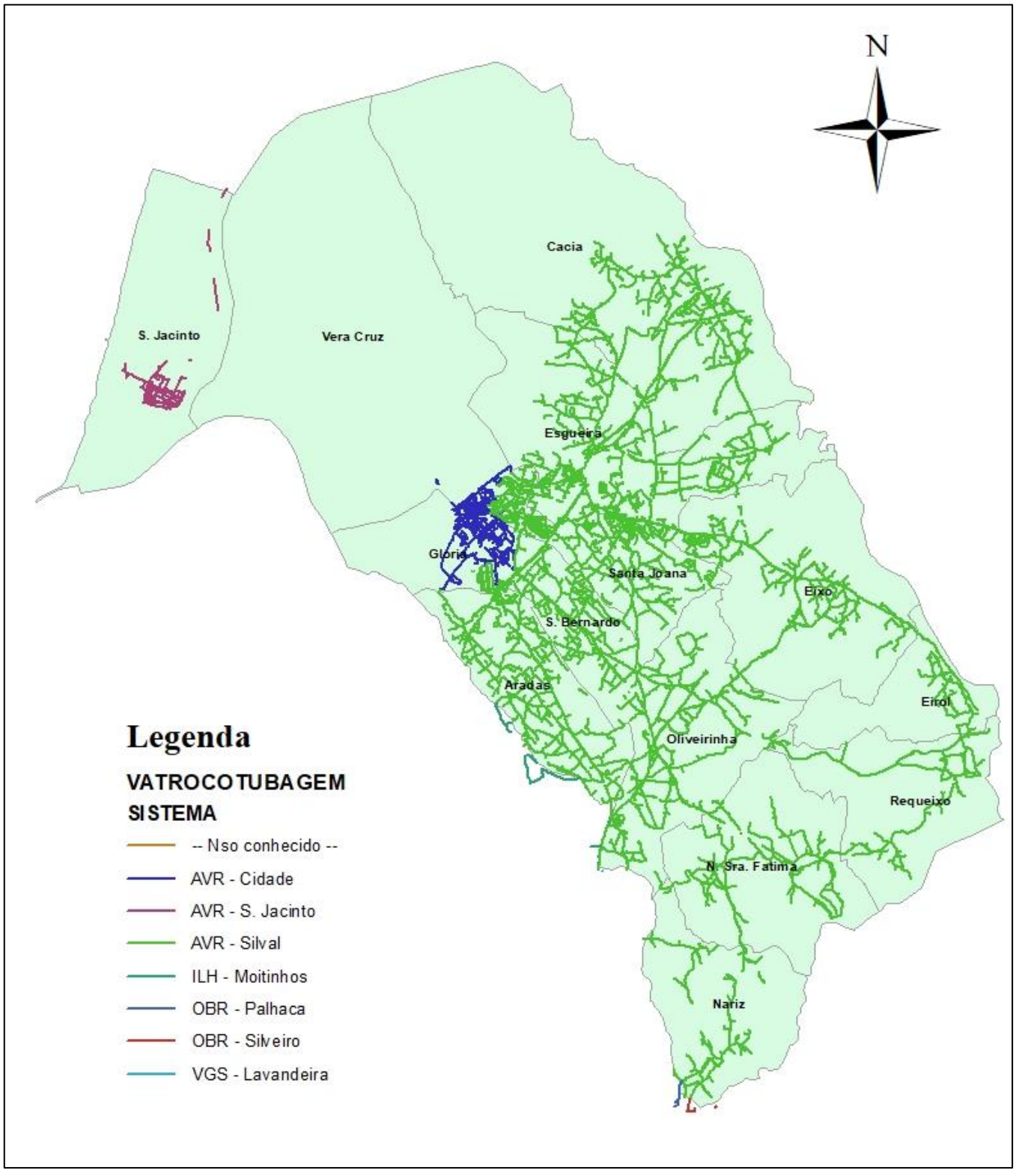
Mapa 4 – Pontos Notáveis, de Captação e de Entrega e Tubagens



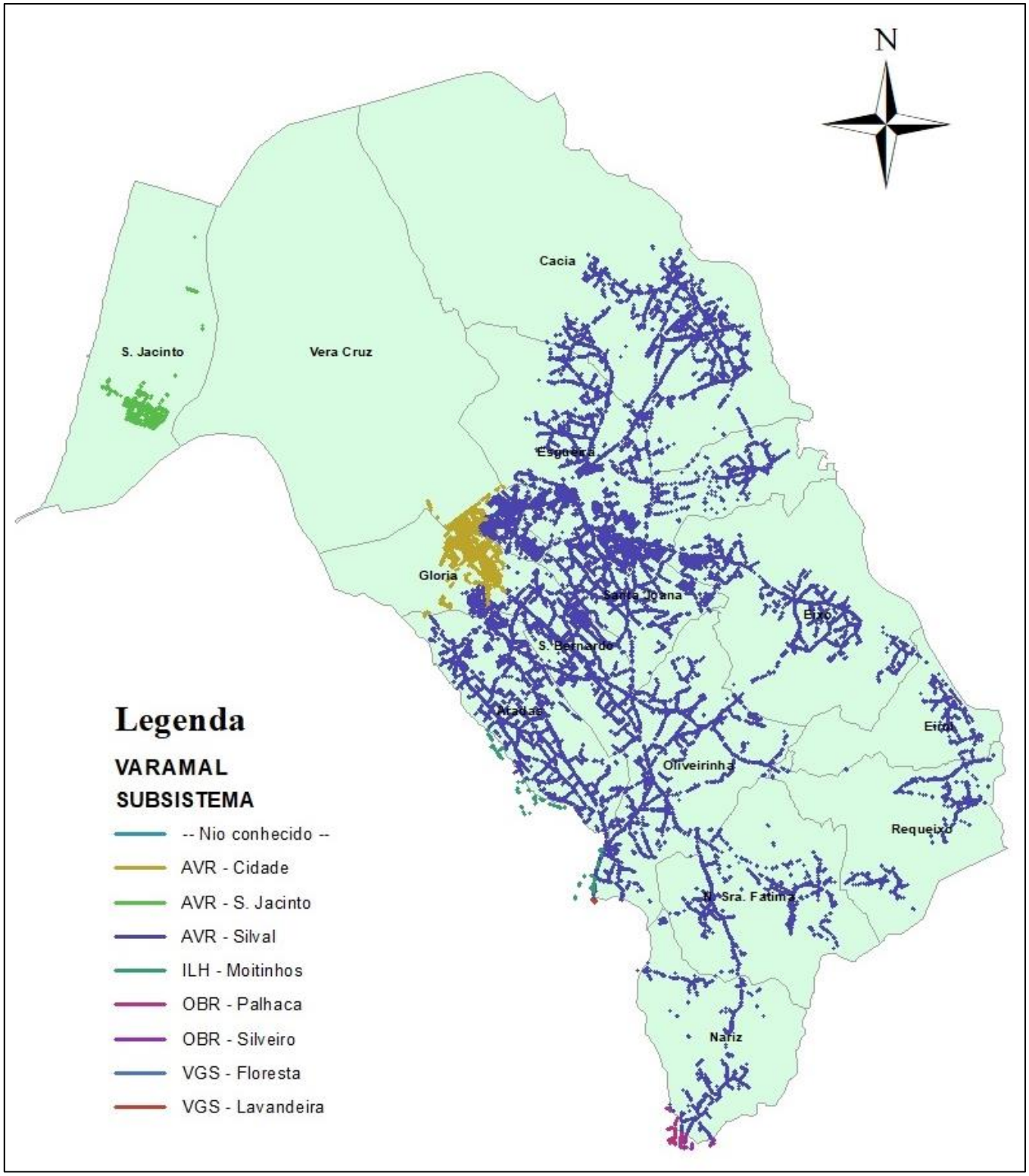
Mapa 5 – Infraestruturas principais



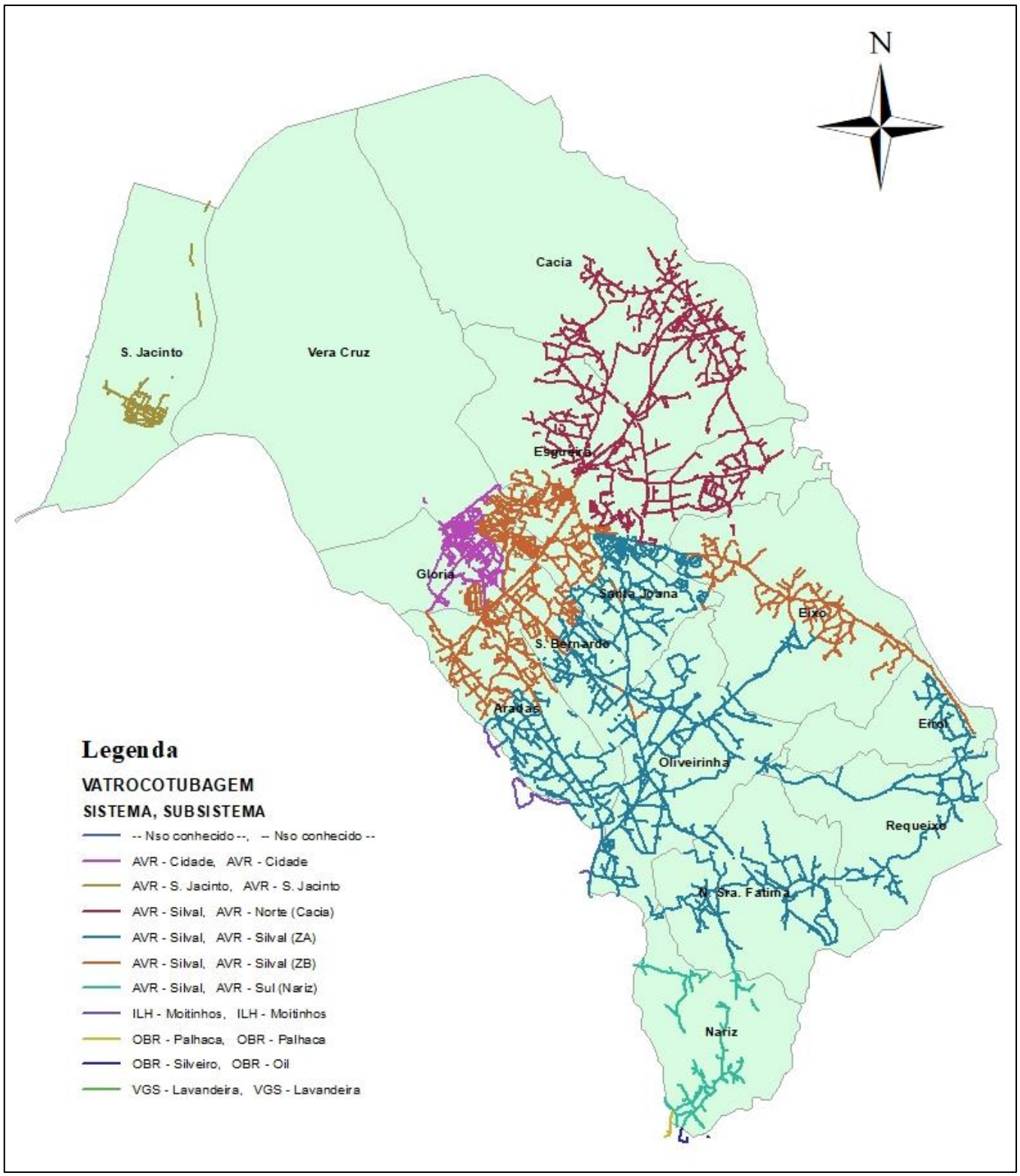
Mapa 6 – Área de Influência – Sistema



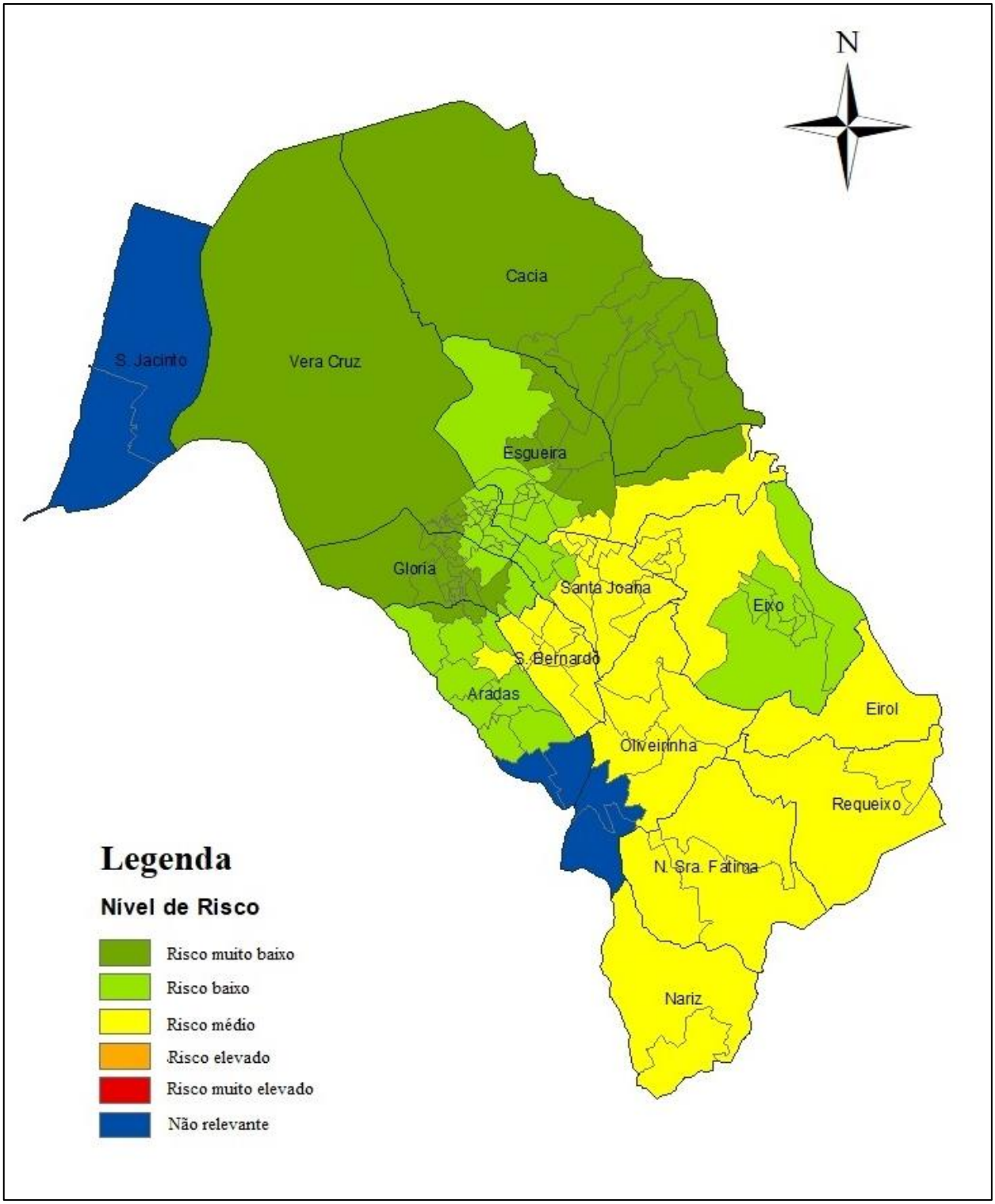
Mapa 7 – Área de Influência – Subsistema



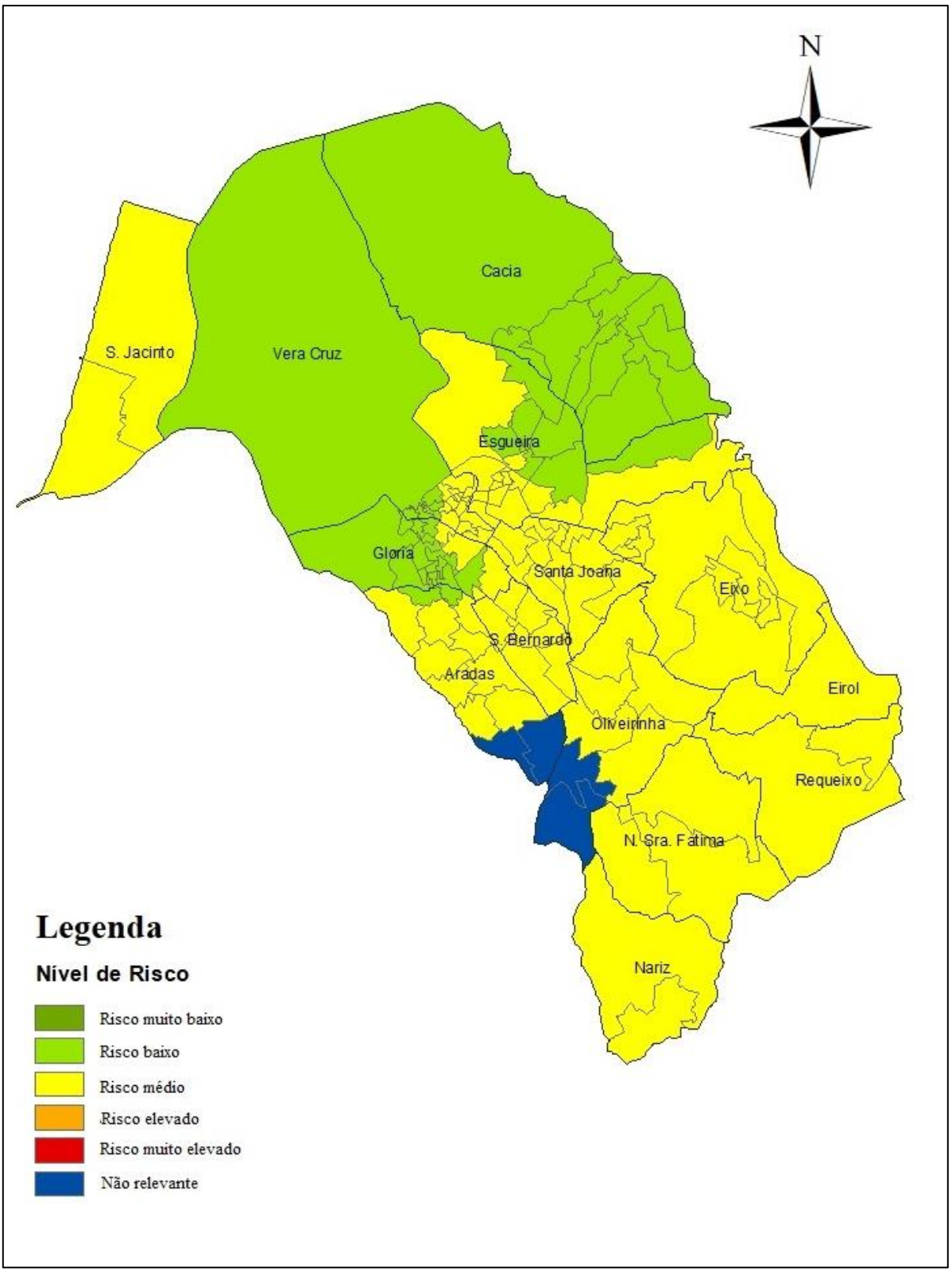
Mapa 8 – Área de Influência – Sistema/Subsistema



Mapa 9 - Mapa de Risco – Silval



Mapa 10 - Mapa de Risco – Rede



Anexo D - *Templates* preenchidos

Parte 1: Ponto de Partida para a Análise

A: Informação Precedente

1. **A análise de risco e vulnerabilidade é preparada pela organização seguinte:**

Data: 2016/2017

2. **Participantes na análise:**

Nome: Manuela Borges

Local de Trabalho:

Universidade de Aveiro

B: Identificação da Funções Críticas e Responsabilidade de Preparação

3. **Qual das funções críticas da sociedade é a organização responsável por garantir e continuar em caso de grandes incidentes e catástrofes?**

Descrever brevemente as funções críticas

A organização é responsável pelo abastecimento de água potável à população do concelho de Aveiro.

4. **Que funções críticas a avaliação de risco e vulnerabilidade cobre?**

Descrever as funções críticas que são com as quais se lida na análise

Abastecimento de água potável ao concelho de Aveiro.

5. **Qual é a razão para o desenvolvimento da análise?**

☒ Nova análise

☐ Análise/Atualização de Rotina

☐ Requerimento Legal

☐ Alterações significativas no que respeita a ameaças

☐ Alterações significativas na organização ou área de responsabilidade

☐ Outras.

Cenário 1 - Falha de Elétrica

Parte 2: Identificação de Ameaças

A: Formular Cenários de Ameaças

1. Que cenários de ameaças podem resultar num impacto negativo substancial nas funções críticas cobertas pela responsabilidade de preparação da empresa?

Devem ser criados um ou mais cenários realistas para serem utilizados na análise. De forma a criar vários cenários copia-se o *template* da parte 2 as vezes necessárias.

Durante a análise a realizar a seguir na Parte 3, é importante avaliar a probabilidade, consequências e vulnerabilidades com base no tema geral de cada cenário (o tipo de incidente) e não nas descrições detalhadas do cenário, como datas, hora do dia ou km², etc.

Número do Cenário: 1	**Título:** Avaria Elétrica – Reservatório Silval
Categoria da Ameaça / Tipo de Incidente	Interrupção/Falha de funções críticas
Resumo dos Eventos	Uma falha no fornecimento de energia elétrica em Oliveirinha afeta o reservatório do Silval.
Extensão Geográfica	Local O concelho de Aveiro, exceto a freguesia de Cacia.
Duração	2 - 7 dias Duração das reservas 4.4 horas
Localização no tempo	Verão Durante Horário Laboral
Aviso	Curto Período de Aviso
Pessoas/Ativos em risco	A interrupção do abastecimento afetaria 77 457 pessoas e as 4 zonas industriais existentes no concelho.
Informação de acontecimentos passados	Incidente imaginado, que pode afetar o sector
Causas diretas que levam à realização do cenário	☒ Fatores naturais ☒ Ações humanas intencionais ☒ Ações humanas não intencionais ☒ Defeito técnico ☐ Erros organizacionais
Informação adicional importante relativa ao cenário	As causas do evento são exteriores à rede de abastecimento em estudo. Na presente análise será considerado o cenário mais desfavorável, ou seja, será considerado que as reservas se esgotam e a duração do evento será uma semana após o tempo que leva essas reservas a esgotar.

Parte 3: Análise dos Cenários de Ameaças

1 – Falha Elétrica

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

A falha elétrica provoca a interrupção do abastecimento de água ao concelho de Aveiro.

Ativar reservas existentes;
Avisar a população da possível interrupção do abastecimento;
Tentar perceber a causa da falha e prever um tempo de duração;

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

1 - Altamente Improvável

Considerar neste contexto:
Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Tendo em conta que não se conhecem incidentes anteriores, considerou-se apenas a plausibilidade do incidente.
Ao considerar o cenário mais desfavorável, supõe-se que as reservas são esgotadas e a falha dura pelo menos mais uma semana. No entanto, a probabilidade duma falha elétrica durar esse tempo é muito baixa.

C: Avaliação de Consequências

Consequências para a organização / área de responsabilidade particular

Quais as consequências do incidente para a organização/área de responsabilidade?

Edifícios e instalações importantes	Falha de equipamentos como bombas elevatórias e estações de tratamento.	4 - Severo
Pessoal e Gestão	Descrever as consequências	Não relevante
Sistemas TI	Falha da telegestão da empresa AdRA que se encontra no recinto do Silval.	4 - Severo
Fornecimento de Energia	A falha do fornecimento de energia consiste no cenário.	Não relevante
Acesso a materiais, bens e serviços essenciais	Limitação de acesso a energia que é essencial ao bom funcionamento da rede de abastecimento.	4 - Severo
Transporte e Distribuição	Interrupção da distribuição de água à população.	4 - Severo
Informação e Comunicação	Não se prevê que a falha afete a comunicação, tendo em conta a tecnologia de hoje.	Não relevante
Outros	Descrever as consequências	Nível de Consequência

Avaliação global das consequências para a organização/área de responsabilidade

Que consequências coletivas teria o incidente na continuação das funções críticas da organização? — 4 - Severo

Inserir comentários

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	Não se prevê que haja perda de vidas, no entanto pode afetar a saúde da população.	3 - Sério
Perda de Ativos (materiais, financeiros, ambientais, etc.)	Perdas financeiras nas indústrias e estabelecimentos ligados à restauração;	2 - Moderado
Ansiedade, insegurança, ira, indignação ou implicações políticas	Ansiedade, ira e indignação da população.	3 - Sério
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Interrupção do abastecimento de água.	3 - Sério

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? — 3 - Sério

Inserir comentários

Avaliação geral de consequências

4 - Severo

Especificar o nível de consequência máximo dos pontos 4 e 6.

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 1 - Altamente Improvável **X consequência** 4 - Severo 4 - Risco baixo

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☐ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, crises;
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de planos de segurança, etc.);
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☐ Edifícios e instalações importantes;
☐ Pessoal e gestão;
☐ Sistemas TI;
☐ Fornecimento de energia;
☐ Acesso a materiais, bens e serviços essenciais;
☐ Transporte/Distribuição;
☐ Informação e comunicação
☒ Outros: Gerador de energia

A segurança, em caso de falha elétrica não é relevante ao cenário.

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 2 - Predominantemente adequado, poucas falhas

Inserir observações

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Pessoal que ativa as reservas existentes;
Pessoal que investiga as causas da falha e estima a duração da mesma;

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 4 - Muitas carências

Inserir observações

Capacidades de recuperação (após o incidente)

1. Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Assim que o fornecimento de energia elétrica seja reativado, a rede funcionará normalmente sem qualquer ação.

Avaliação geral das capacidades de recuperação

2. **Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente?** 1 - Adequado

Inserir observações

Cenário 2 – Sismo

Parte 2: Identificação de Ameaças

A: Formular Cenários de Ameaças

Número do Cenário: 2	**Título:** Sismo – Intensidade 7
Categoria da Ameaça / Tipo de Incidente	Desastres Naturais
Resumo dos Eventos	Um sismo com intensidade 7, na escala de Mercalli Modificada, afeta Aveiro.
Extensão Geográfica	Nacional O sismo afeta todo o país com intensidades distintas.
Duração	0 - 1 dia Os sismos têm durações muito curtas (poucos segundos a poucas dezenas de segundos (IPMA, 2017).
Localização no tempo	Verão Altura da Semana
Aviso	Nenhum Aviso Um sismo é um evento imprevisto o que faz com que seja impossível avisar a população.
Pessoas/Ativos em risco	O sismo afeta toda a população de Aveiro, cerca de 78.450 habitantes. Alvenarias podem sofrer algumas fraturas. Ondulação nos tanques.
Informação de acontecimentos passados	Inf. Acont. Pass. Intensidade determinada tendo em conta sismos que aconteceram no passado nomeadamente o sismo de 1755 e 1969.
Causas diretas que levam à realização do cenário	☒ Fatores naturais ☐ Ações humanas intencionais ☐ Ações humanas não intencionais ☐ Defeito técnico ☐ Erros organizacionais
Informação adicional importante relativa ao cenário	Dificuldade em permanecer de pé, notado por condutores de automóveis, objetos pendurados tremem, mobílias partem, verificação de danos em alvenarias do tipo D, incluindo fraturas, chaminés partem ao nível das coberturas, queda de reboco, tijolos soltos, pedras, telhas, cornijas, parapeitos soltos e ornamentos arquitetónicos, algumas fraturas em alvenarias tipo C, ondas nos tanques, água turva com lodo, pequenos desmoronamentos e abatimentos ao longo das margens de areia e de cascalho, os sinos grandes tocam e os diques de betão armado para irrigação são danificados.

Parte 3: Análise dos Cenários de Ameaças

Cenário 2 - Sismo

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

Descrever tarefas operacionais particularmente importantes
Manter o abastecimento de água potável;

Descrever tarefas de gestão de crises
Analisar a rede e identificar possíveis danos causados pelo sismo;
Se necessário, avisar a população da interrupção do abastecimento e sua duração para reparação de possíveis danos;
Reparação rápida e eficaz dos danos causados pelo sismo;
Garantir abastecimento a edifícios e instalações importantes como hospitais e centros de saúde.

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

3 - Provável

Considerar neste contexto:
Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Descrever os antecedentes para a avaliação da probabilidade
Tendo em conta a sismicidade em Portugal, nomeadamente a análise de ocorrências passadas como o sismo de 1755 e o sismo de 1969, considera-se provável a ocorrência de sismos em Portugal no futuro.
No que toca à plausibilidade, um sismo é um evento muito plausível visto que existe informações de ocorrências no passado.

Consequências para a organização / área de responsabilidade particular **Quais as consequências do incidente para a organização/área de responsabilidade?**		
Edifícios e instalações importantes	Os edifícios importantes, como reservatórios, devem ser dimensionados tendo em consideração a ocorrência de sismos. Caso isso aconteça, não se espera que um sismo no concelho de Aveiro afete os reservatórios ou outros edifícios importantes da rede.	1 - Limitado
Pessoal e Gestão	O sismo pode assustar as pessoas tendo em conta que o mesmo pode provocar dificuldade em permanecer de pé, os condutores de automóveis sentem, objetos pendurados tremem e alvenarias podem sofrer fraturas.	2 - Moderado
Sistemas TI	Não se espera que o sismo afete a telegestão diretamente, no entanto pode provocar danos em serviços das quais esta depende, como energia elétrica.	2 - Moderado
Fornecimento de Energia	Pode ser cortado devido a danos na rede de fornecimento de energia.	2 - Moderado
Acesso a materiais, bens e serviços essenciais	Fornecimento de energia elétrica pode ser afetado pelo sismo.	2 - Moderado
Transporte e Distribuição	Condutas, tubagens ou ramais podem ser danificados pelo sismo, provocando a interrupção do abastecimento à área de influência do elemento danificado.	2 - Moderado
Informação e Comunicação	Não se esperam consequências a nível de informação e comunicação	Não relevante
Outros	Descrever as consequências	Nível de Consequência
Avaliação global das consequências para a organização/área de responsabilidade Que consequências coletivas teria o incidente na continuação das funções críticas da organização? Inserir comentários		2 - Moderado

C: Avaliação de Consequências

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	O pânico pode provocar perdas de vida e saúde na população.	4 - Severo
Perda de Ativos (materiais, financeiros, ambientais, etc.)	Perdas financeiras devido a estragos	1 - Limitado
Ansiedade, insegurança, ira, indignação ou implicações políticas	Ansiedade e insegurança devido ao pânico que pode resultar de um sismo percetível pelo Homem.	4 - Severo
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Danos nas infraestruturas críticas, mínimos ou inexistentes	3 - Sério

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? 4 - Severo

Sabendo os efeitos do sismo com intensidade 7, descritos na parte 2, os efeitos visíveis do sismo como não se ser capaz de ficar de pé, objetos pendurados a abanar, condutores de automóveis sentirem pode provocar o pânico e por consequência afetar o discernimento da população levando a acidentes, como perdas de vida.

Avaliação geral de consequências

4 - Severo

Especificar o nível de consequência máximo dos pontos 4 e 6.

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 3 - Provável **X consequência** 4 - Severo 12 - Risco médio

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☐ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, planos de segurança, etc.);
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de crises;
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações

Existe informação disponível no site da proteção civil e na internet em geral relativa a forma como agir em caso de ocorrência de sismo.
O tema dos sismos em Portugal tem vindo a ser muito debatido nos últimos anos, sendo que existe a tentativa de sensibilizar a população para o tema.
Estas preparações não são da empresa em si, mas de entidades como proteção civil, universidades, em termos de investigação, o LNEC e a comunidade de engenheiros civis em geral.

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☒ Edifícios e instalações importantes;
☐ Pessoal e gestão;
☐ Sistemas TI;
☒ Fornecimento de energia;
☒ Acesso a materiais, bens e serviços essenciais;
☐ Transporte/Distribuição;
☐ Informação e comunicação
☐ Outros.

Descrever as medidas preventivas ou de mitigação dos estragos

Não é possível prevenir um sismo, no entanto é possível proteger os edifícios importantes e o fornecimento de energia, que consiste num serviço essencial à rede de abastecimento, através da consideração da ocorrência do mesmo no dimensionamento e na construção/instalação das redes.

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 5 - Altamente inadequado

Inserir observações

Na presente análise considera-se que não existe preparação da empresa através de planeamento. No entanto, nos últimos anos tem havido um esforço para a sensibilização da população para a possível ocorrência de sismos, havendo muita informação disponível.

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Pessoal que analisa a rede e identifica possíveis danos;
Pessoal de manutenção que repara os danos;
Bombeiros Voluntário e Municipais;
Proteção Civil;
Piquetes

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 2 - Predominantemente adequado, poucas falhas

Inserir observações

Capacidades de recuperação (após o incidente)

Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Pessoal de manutenção que repara os danos;

Avaliação geral das capacidades de recuperação

Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente? 2 - Predominantemente adequado, poucas falhas

Inserir observações

Cenário 3 – Avaria Comunicação e TI (Telegestão)

Parte 2: Identificação de Ameaças

A: Formular Cenários de Ameaças

Número do Cenário: 3	**Título:** Falha do sistema de telegestão
Categoria da Ameaça / Tipo de Incidente	Interrupção/Falha de funções críticas
Resumo dos Eventos	Ocorre uma falha do sistema de telegestão que pode ter várias causas, nomeadamente interrupção da internet ou falha elétrica. A falha da telegestão impede o acesso a informação relativa à rede, como caudais instantâneos, pressões, níveis de água, etc.
Extensão Geográfica	Local A falha da telegestão ocorre no Silval, no entanto afeta toda a rede tendo em conta que a telegestão engloba toda a rede em estudo.
Duração	0 - 1 dia
Localização no tempo	Verão Altura da Semana
Aviso	Curto Período de Aviso A telegestão é responsável pelo controlo e monitorização da rede, pelo que a avaria da mesma pode provocar problemas de pressão ou caudal. Assim, é necessário informar a população das consequências que possam ocorrer.
Pessoas/Ativos em risco	A avaria da telegestão afeta a rede que abastece os 78450 habitantes da cidade de Aveiro.
Informação de acontecimentos passados	Incidente imaginado, que pode afetar o sector
Causas diretas que levam à realização do cenário	☒ Fatores naturais ☒ Ações humanas intencionais ☒ Ações humanas não intencionais ☒ Defeito técnico ☐ Erros organizacionais
Informação adicional importante relativa ao cenário	

Parte 3: Análise dos Cenários de Ameaças

3 – Falha do sistema da telegestão

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

Descrever tarefas operacionais particularmente importantes

A telegestão permite a monitorização e controlo, em tempo real do sistema. Assim, a falha desse sistema resultaria na impossibilidade de aceder à informação da rede. No caso de existir alguma anomalia em algum elemento da rede, como estações elevatórias, condutas, estações de tratamento, o problema só seria identificado quando afeta-se a população.

Descrever tarefas de gestão de crises

Conhecer as causas da falha do sistema;
Solucionar os problemas que causaram a falha;
Avisar a população das possíveis falhas na distribuição, como falta de pressão da água;

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

3 - Provável

Considerar neste contexto:

Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Descrever os antecedentes para a avaliação da probabilidade

Em termos de frequência, não são conhecidos eventos passados. No entanto, considera-se que a probabilidade da ocorrência do evento é 3 - Provável pois considera-se plausível a interrupção da internet ou um possível erro do próprio sistema informático.

C: Avaliação de Consequências

Consequências para a organização / área de responsabilidade particular

Quais as consequências do incidente para a organização/área de responsabilidade?

Edifícios e instalações importantes	Se bombas elevatórias ou estações de tratamento deixarem de funcionar devidamente, essa informação não é conhecida automaticamente.	4 - Severo
Pessoal e Gestão	Não se prevê que afete as pessoas. No entanto, afeta a gestão tendo em conta que a gestão é feita em tempo real através do sistema que falha no incidente.	3 - Sério
Sistemas TI	A falha dos sistemas TI corresponde ao cenário.	Não relevante
Fornecimento de Energia	Pode ser uma causa. Não existem consequências para a mesma.	Não relevante
Acesso a materiais, bens e serviços essenciais	Não se prevê que seja impedido o acesso.	Não relevante
Transporte e Distribuição	A distribuição de água pode ser condicionada podendo haver problemas de pressão;	2 - Moderado
Informação e Comunicação	Não se prevê que afeta a comunicação, mas afeta a informação elativa à rede.	3 - Sério
Outros	Descrever as consequências	Nível de Consequência

Avaliação global das consequências para a organização/área de responsabilidade

Que consequências coletivas teria o incidente na continuação das funções críticas da organização? 4 - Severo

Inserir comentários

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	Não se prevê perdas de vida ou saúde	Não relevante
Perda de Ativos (materiais, financeiros, ambientais, etc.)	Não se prevê perdas de ativos.	Não relevante
Ansiedade, insegurança, ira, indignação ou implicações políticas	O possível decréscimo da qualidade de abastecimento, p.ex. pressão da água, pode provocar descontentamento, indignação e ira.	2 - Moderado
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Não se prevê a interrupção de qualquer infraestrutura crítica;	Não relevante

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? — 2 - Moderado

Inserir comentários

Avaliação geral de consequências

4 - Severo

Especificar o nível de consequência máximo dos pontos 4 e 6.

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 3 - Provável **X consequência** 4 - Severo 12 - Risco médio

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☐ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, planos de segurança, etc.);
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de crises;
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações

Na presente análise considera-se que não existe preparação através de planeamento.

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☐ Edifícios e instalações importantes;
☐ Acesso a materiais, bens e serviços essenciais;
☒ Pessoal e gestão;
☐ Transporte/Distribuição;
☐ Sistemas IT;
☐ Informação e comunicação
☐ Fornecimento de energia;
☐ Outros: Gerador

Descrever as medidas preventivas ou de mitigação dos estragos

Em caso de falha da internet, considera-se que não existem medidas.

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 3 - Algumas falhas graves

Inserir observações

Não existem medidas para prevenir ou mitigar as consequências da falha da internet;

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Sugere-se que se realizem acordos com empresas de telecomunicações que garantam o acesso à internet em caso de falha

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 3 - Algumas falhas graves

Inserir observações

Capacidades de recuperação (após o incidente)

Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Não se aplica visto que assim que a ligação à internet seja restaurada o sistema funcionará normalmente. Não se prevê que a falha de internet provoque danos físicos na rede.

Avaliação geral das capacidades de recuperação

Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente? Não se sabe

Inserir observações

Cenário 4 - Avaria na Rede de Abastecimento de Água – Avaria de bombas doseadoras de hipoclorito de sódio

Parte 2: Identificação de Ameaças

A: Formular Cenários de Ameaças

Número do Cenário: 4	**Título:** Avaria na rede de abastecimento – Bombas doseadoras
Categoria da Ameaça / Tipo de Incidente	Interrupção/Falha de funções críticas
Resumo dos Eventos	Ocorre uma avaria nas bombas doseadora de hipoclorito de sódio, que deixa de garantir a qualidade da água.
Extensão Geográfica	Local O reservatório do Silval afeta a maioria da população de Aveiro.
Duração	0 - 1 dia A intervenção para consertar as bombas doseadoras é considerada urgente pela AdRA pelo que não se espera que a avaria dure um longo período de tempo.
Localização no tempo	Verão Altura da Semana
Aviso	Nenhum Aviso
Pessoas/Ativos em risco	Sendo que a avaria dura um curto período de tempo e que, em principio não é necessário interromper o abastecimento, o cenário não afeta a população.
Informação de acontecimentos passados	Incidente imaginado, que pode afetar o sector
Causas diretas que levam à realização do cenário	☐ Fatores naturais ☐ Ações humanas intencionais ☐ Ações humanas não intencionais ☒ Defeito técnico ☐ Erros organizacionais
Informação adicional importante relativa ao cenário	

Parte 3: Análise dos Cenários de Ameaças

Avaria na rede de abastecimento – Avaria bombas doseadoras de hipoclorito de sódio

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

Descrever tarefas operacionais particularmente importantes
Identificar a avaria;
Mobilizar esforços para reparação da avaria.

Descrever tarefas de gestão de crises
Não se prevê que ocorra algum tipo de crise

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

4 - Bastante Provável

Considerar neste contexto:
Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Descrever os antecedentes para a avaliação da probabilidade
Não existem informações de acontecimentos passados para considerar a frequência.
O incidente pode acontecer tendo em conta que as bombas doseadoras são dispositivos com tempos de vida limitados.

C: Avaliação de Consequências

Consequências para a organização / área de responsabilidade particular

Quais as consequências do incidente para a organização/área de responsabilidade?

Edifícios e instalações importantes	Descrever as consequências	Não relevante
Pessoal e Gestão	Gestão deve proceder à reparação da avaria	1 - Limitado
Sistemas IT	Descrever as consequências	Não relevante
Fornecimento de Energia	Descrever as consequências	Não relevante
Acesso a materiais, bens e serviços essenciais	O hipoclorito de sódio é um bem essencial para a garantia da qualidade da água.	3 - Sério
Transporte e Distribuição	Descrever as consequências	Não relevante
Informação e Comunicação	Descrever as consequências	Não relevante
Outros	Descrever as consequências	Nível de Consequência

Avaliação global das consequências para a organização/área de responsabilidade

Que consequências coletivas teria o incidente na continuação das funções críticas da organização? 3 - Sério

Inserir comentários

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	Descrever as consequências	Não relevante
Perda de Ativos (materiais, financeiros, ambientais, etc.)	Descrever as consequências	Não relevante
Ansiedade, insegurança, ira, indignação ou implicações políticas	Descrever as consequências	Não relevante
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Descrever as consequências	Não relevante

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? Não relevante

Inserir comentários

Tendo em conta que os níveis de hipoclorito de sódio adicionado à água diminuem gradualmente não se espera que a avaria das bombas doseadoras afete a população.

Avaliação geral de consequências

3 - Sério

Especificar o nível de consequência máximo dos pontos 4 e 6.

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 4 - Bastante Provável **X consequência** 3 - Sério 12 - Risco médio

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☐ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, planos de segurança, etc.);
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de crises;
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações

Na presente análise não se considera que existe preparação através de planeamento

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☐ Edifícios e instalações importantes;
☒ Pessoal e gestão;
☐ Sistemas IT;
☐ Fornecimento de energia;
☐ Acesso a materiais, bens e serviços essenciais;
☐ Transporte/Distribuição;
☐ Informação e comunicação
☐ Outros.

Descrever as medidas preventivas ou de mitigação dos estragos

A segurança não é relevante no presente cenário. No entanto, a telegestão da empresa AdRA identifica a avaria. Tendo em conta que essa avaria é considerada urgente para a AdRA o tempo de resposta de recuperação é muito reduzido.

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 2 - Predominantemente adequado, poucas falhas

Inserir observações

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Gestão identifica a falha e mobiliza meios necessários para a reparação da avaria.

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 2 - Predominantemente adequado, poucas falhas

Inserir observações

Capacidades de recuperação (após o incidente)

Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Pessoal que monitoriza os níveis de hipoclorito de sódio de forma a garantir a qualidade da água abastecida.

Avaliação geral das capacidades de recuperação

Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente? 1 - Adequado

Inserir observações

Cenário 5 – Crime

a) Ataque cibernético aos Sistemas TI (telegestão)

Parte 2: Identificação de Ameaças
A: Formular Cenários de Ameaças

Número do Cenário: 5	**Título: a)** Ataque cibernético aos sistemas TI (telegestão)
Categoria da Ameaça / Tipo de Incidente	Outras ameaças Criminalidade
Resumo dos Eventos	Um ataque aos sistemas TI impende o acesso da AdRA à informação da rede, o que resulta na perda de controlo da mesma. Concede ainda o controlo da rede à (s) pessoa (s) que forem responsáveis pelo ataque.
Extensão Geográfica	Não relevante
Duração	2 - 7 dias (arbitrado)
Localização no tempo	Verão Não Relevante
Aviso	Longo Período de Aviso Aviso à população relativa a possível interrupção do abastecimento devido ao ataque cibernético.
Pessoas/Ativos em risco	O ataque afeta toda a rede e, por consequência, toda a população da cidade de Aveiro, 78450 habitantes, estabelecimentos ligados à alimentação, zonas industriais, equipamentos de saúde, governo, proteção civil. O ataque pode por em causa a própria rede tendo em conta que as pressões e caudais da mesma podem ser alterados.
Informação de acontecimentos passados	Incidente imaginado, que pode afetar o sector
Causas diretas que levam à realização do cenário	☐ Fatores naturais ☒ Ações humanas intencionais ☐ Ações humanas não intencionais ☐ Defeito técnico ☐ Erros organizacionais
Informação adicional importante relativa ao cenário	

Parte 3: Análise dos Cenários de Ameaças

5 – a) Ataque cibernético aos sistema TI (telegestão)

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

Descrever tarefas operacionais particularmente importantes
Retomar controlo dos sistemas e garantir abastecimento à população;

Descrever tarefas de gestão de crises
Contactar as autoridades competentes para identificação da(s) pessoa(s) responsável pelo ataque;
Aviso à população de possíveis consequências do ataque;

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

1 - Altamente Improvável

Considerar neste contexto:
Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Descrever os antecedentes para a avaliação da probabilidade
Não existem acontecimentos passados que permitam determinar frequência para o acontecimento;

C: Avaliação de Consequências

Consequências para a organização / área de responsabilidade particular

Quais as consequências do incidente para a organização/área de responsabilidade?

Edifícios e instalações importantes	Pode afetar bombas elevatórias ou elementos da rede como tubagens devido à alteração de caudais e pressões. Possíveis danos físicos na rede.	3 - Sério
Pessoal e Gestão	Não seria possível gerir a rede.	3 - Sério
Sistemas TI	O ataque aos sistemas TI corresponde ao cenário.	Não relevante
Fornecimento de Energia	Fornecimento de energia externo à rede	Não relevante
Acesso a materiais, bens e serviços essenciais	Descrever as consequências	Não relevante
Transporte e Distribuição	O ataque pode ter como objetivo interromper o abastecimento.	4 - Severo
Informação e Comunicação	Manipulação da telegestão pode fornecer informações falsas relativas à rede.	4 - Severo
Outros	Descrever as consequências	Nível de Consequência

Avaliação global das consequências para a organização/área de responsabilidade

Que consequências coletivas teria o incidente na continuação das funções críticas da organização? — 4 - Severo

Inserir comentários

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	Dependendo da duração, pode afetar a saúde da população.	4 - Severo
Perda de Ativos (materiais, financeiros, ambientais, etc.)	Perdas financeiras devido à interrupção do abastecimento.	2 - Moderado
Ansiedade, insegurança, ira, indignação ou implicações políticas	Dependendo da duração, pode afetar o ânimo dos habitantes	3 - Sério
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Pode ser o objetivo do ataque	4 - Severo

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? — 4 - Severo

Inserir comentários

Avaliação geral de consequências

Especificar o nível de consequência máximo dos pontos 4 e 6. — 4 - Severo

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 1 - Altamente Improvável **X** **consequência** 4 - Severo 4 - Risco baixo

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☐ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, planos de segurança, etc.);
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de crises;
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações

Na presente análise não se considera que existe preparação através de planeamento

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☐ Edifícios e instalações importantes;
☐ Pessoal e gestão;
☐ Sistemas IT;
☐ Fornecimento de energia;
☐ Acesso a materiais, bens e serviços essenciais;
☐ Transporte/Distribuição;
☐ Informação e comunicação
☐ Outros.

Descrever as medidas preventivas ou de mitigação dos estragos

A segurança dos elementos descritos não é relevante neste cenário, exceto no caso dos sistemas TI.

Não se conhece as medidas de segurança dos sistemas TI da empresa pelo que se considera que não existem.

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 5 - Altamente inadequado

Inserir observações

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Não se conhece as capacidades de resposta e alívio na eventualidade de ocorrência de um ataque aos sistemas TI da empresa pelo que se considera que não existem.

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 5 - Altamente inadequado

Inserir observações

Capacidades de recuperação (após o incidente)

Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Não se conhece as capacidades de resposta e alívio na eventualidade de ocorrência de um ataque aos sistemas TI da empresa pelo que se considera que não existem.

Avaliação geral das capacidades de recuperação

Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente? 4 - Muitas carências

Inserir observações

No caso de danos físicos na rede, existe o departamento de manutenção que será mobilizado de forma a reparar eventuais danos.

Cenário 5 – Crime

b) Vandalismo/Sabotagem - Destruição do Reservatório do Silval responsável pela distribuição da água fornecido pelo Carvoeiro

Parte 2: Identificação de Ameaças

A: Formular Cenários de Ameaças

Número do Cenário: 5	**Título: b)** Vandalismo/Sabotagem - Destruição do Reservatório do Silval responsável pela distribuição da água fornecido pelo Carvoeiro
Categoria da Ameaça / Tipo de Incidente	Interrupção/Falha de funções críticas
Resumo dos Eventos	
Extensão Geográfica	Local Concelho de Aveiro
Duração	1 - 4 semanas Reconstrução do reservatório
Localização no tempo	Verão Não Relevante
Aviso	Longo Período de Aviso A destruição do reservatório em questão interrompe o abastecimento durante um longo período de tempo por isso a população tem que ser avisada dessa interrupção.
Pessoas/Ativos em risco	77457 habitantes, zonas industriais, estabelecimentos ligados à restauração, equipamentos de saúde, governo, educação, etc.
Informação de acontecimentos passados	Incidente imaginado, que pode afetar o sector
Causas diretas que levam à realização do cenário	☐ Fatores naturais ☒ Ações humanas intencionais ☐ Ações humanas não intencionais ☐ Defeito técnico ☐ Erros organizacionais
Informação adicional importante relativa ao cenário	

Parte 3: Análise dos Cenários de Ameaças

5 b) Vandalismo/Sabotagem - Destruição do Reservatório do Silval responsável pela distribuição da água fornecido pelo Carvoeiro

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

Descrever tarefas operacionais particularmente importantes

Descrever tarefas de gestão de crises
Ativar reservas;
Analisar duração de interrupção do abastecimento;
Aviso à população;
Desenvolver soluções para garantir acesso da população e equipamentos importantes a água potável;

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

1 - Altamente Improvável

Considerar neste contexto:
Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Descrever os antecedentes para a avaliação da probabilidade
Não existem eventos anteriores que permitam a determinação de frequência.
A destruição do reservatório é um incidente com execução difícil.

C: Avaliação de Consequências

Consequências para a organização / área de responsabilidade particular

Quais as consequências do incidente para a organização/área de responsabilidade?

Edifícios e instalações importantes	Destruição de edifícios importantes é o cenário.	Não relevante
Pessoal e Gestão	Pode afetar pessoas que se encontrem no local.	4 - Severo
Sistemas IT	Não se prevê que afete os sistemas	1 - Limitado
Fornecimento de Energia	Descrever as consequências	Não relevante
Acesso a materiais, bens e serviços essenciais	Impede acesso ao abastecimento do Carvoeiro	4 - Severo
Transporte e Distribuição	Descrever as consequências	Não relevante
Informação e Comunicação	Não se prevê que afete a informação ou a comunicação	1 - Limitado
Outros	Descrever as consequências	Nível de Consequência

Avaliação global das consequências para a organização/área de responsabilidade

Que consequências coletivas teria o incidente na continuação das funções críticas da organização? 4 - Severo

Inserir comentários

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	Pode afetar a saúde das pessoas	4 - Severo
Perda de Ativos (materiais, financeiros, ambientais, etc.)	Perdas financeiras de estabelecimentos e zonas industriais	3 - Sério
Ansiedade, insegurança, ira, indignação ou implicações políticas	A interrupção do abastecimento afeta o ânimo das pessoas	3 - Sério
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Interrupção do abastecimento de água	4 - Severo

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? 4 - Severo

Inserir comentários

Avaliação geral de consequências

4 - Severo

Especificar o nível de consequência máximo dos pontos 4 e 6.

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 1 - Altamente Improvável **X** **consequência** 4 - Severo 4 - Risco baixo

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☐ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, planos de segurança, etc.);
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de crises;
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações
Na presente análise que não existe preparação através de planeamento

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☐ Edifícios e instalações importantes;
☐ Pessoal e gestão;
☐ Sistemas IT;
☐ Fornecimento de energia;
☐ Acesso a materiais, bens e serviços essenciais;
☐ Transporte/Distribuição;
☐ Informação e comunicação
☐ Outros.

Descrever as medidas preventivas ou de mitigação dos estragos
Recinto dos reservatórios encontra-se vedados;
Localização de difícil acesso;

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 3 - Algumas falhas graves

Inserir observações

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Bombeiros;
Equipamento de Justiça: GNR, PSP
Pessoal para ativar reservas, analisar o impacto na rede, desenvolver soluções;

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 2 - Predominantemente adequado, poucas falhas

Inserir observações

Capacidades de recuperação (após o incidente)

Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Não se sabe

Avaliação geral das capacidades de recuperação

Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente? Não se sabe

Inserir observações

Cenário 5 – Crime
c) Vandalismo/Sabotagem – Contaminação da Água

Parte 2: Identificação de Ameaças

A: Formular Cenários de Ameaças

Número do Cenário: 5	**Título: c)** Vandalismo/Sabotagem – Contaminação da Água
Categoria da Ameaça / Tipo de Incidente	Doenças e Epidemias
Resumo dos Eventos	Contaminação da água devido a danos intencionais no sistema de adição de hipoclorito de sódio ou contaminantes adicionados intencionalmente.
Extensão Geográfica	Local Concelho de Aveiro
Duração	2 - 7 dias Duração corresponde ao tempo necessário para descontaminar a rede.
Localização no tempo	Verão Fins de semana/Feriados
Aviso	Longo Período de Aviso No que toca a uma contaminação o aviso à população deve ser rápido e eficiente de forma a diminuir o máximo possível o número de pessoas afetadas.
Pessoas/Ativos em risco	A população da cidade de Aveiro, exceto a freguesia de São Jacinto. Equipamentos de ensino, justiça, governo, etc. e serviços como estabelecimentos ligados à restauração.
Informação de acontecimentos passados	Incidente imaginado, que pode afetar o sector
Causas diretas que levam à realização do cenário	☐ Fatores naturais ☒ Ações humanas intencionais ☐ Ações humanas não intencionais ☐ Defeito técnico ☐ Erros organizacionais
Informação adicional importante relativa ao cenário	

Parte 3: Análise dos Cenários de Ameaças

Cenário 5 – Crime **c)** Vandalismo/Sabotagem – Contaminação da Água

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

Descrever tarefas operacionais particularmente importantes
Interromper o abastecimento;

Descrever tarefas de gestão de crises
Comunicar a contaminação à população e equipamentos de saúde e educação;
Desenvolver planos para abastecer equipamentos de saúde para ser possível tratar pessoas contaminadas;
Desenvolver planos para abastecer a população;
Proceder à descontaminação da rede de abastecimento;

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

1 - Altamente Improvável

Considerar neste contexto:
Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Descrever os antecedentes para a avaliação da probabilidade
Não existem acontecimentos passados que permitam determinar frequência.
Os reservatórios encontram-se vedados e fechados e o controlo da água é realizado em tempo real. Teria que haver algum problema em termos de telegestão para que a contaminação não fosse detetada antes da água ser abastecida.

C: Avaliação de Consequências

Consequências para a organização / área de responsabilidade particular

Quais as consequências do incidente para a organização/área de responsabilidade?

Edifícios e instalações importantes	Sabotagem de equipamentos existentes nos reservatórios, equipamentos de adição de hipoclorito de sódio;	3 - Sério
Pessoal e Gestão	Descrever as consequências	Não relevante
Sistemas IT	Descrever as consequências	Não relevante
Fornecimento de Energia	Descrever as consequências	Não relevante
Acesso a materiais, bens e serviços essenciais	Descrever as consequências	Não relevante
Transporte e Distribuição	Descrever as consequências	Não relevante
Informação e Comunicação	Descrever as consequências	Não relevante
Outros	Descrever as consequências	Nível de Consequência

Avaliação global das consequências para a organização/área de responsabilidade

Que consequências coletivas teria o incidente na continuação das funções críticas da organização? Não relevante

Inserir comentários

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	Afeta a saúde, sendo possível haver perdas de vidas;	5 - Crítico
Perda de Ativos (materiais, financeiros, ambientais, etc.)	A contaminação pode afetar o ambiente. Perdas financeiras devido à interrupção do abastecimento	4 - Severo
Ansiedade, insegurança, ira, indignação ou implicações políticas	Afeta o ânimo das pessoas	4 - Severo
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Interrupção do abastecimento de água	4 - Severo

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? 5 - Crítico

Inserir comentários

Avaliação geral de consequências

5 - Crítico

Especificar o nível de consequência máximo dos pontos 4 e 6.

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 1 - Altamente Improvável **X consequência** 5 - Crítico 5 - Risco baixo

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☐ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, planos de segurança, etc.);
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de crises;
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações

Na presente análise que não existe preparação através de planeamento

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☐ Edifícios e instalações importantes;
☐ Pessoal e gestão;
☐ Sistemas IT;
☐ Fornecimento de energia;
☐ Acesso a materiais, bens e serviços essenciais;
☐ Transporte/Distribuição;
☐ Informação e comunicação
☐ Outros.

Descrever as medidas preventivas ou de mitigação dos estragos

Controlo de qualidade e água

Segurança de edifícios é importante tendo em conta que é necessária presença física para contaminar o abastecimento.

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 3 - Algumas falhas graves

Inserir observações

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Bombeiros;
Proteção Civil;
Equipamentos de Justiça: GNR, PSP

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 3 - Algumas falhas graves

Inserir observações

Capacidades de recuperação (após o incidente)

Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Avaliação geral das capacidades de recuperação

Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente? Não se sabe

Inserir observações

Cenário 6 – Falha no Carvoeiro

Parte 2: Identificação de Ameaças

A: Formular Cenários de Ameaças

Número do Cenário: 6	**Título:** Falha do Carvoeiro – Interrupção do fornecimento do Carvoeiro
Categoria da Ameaça / Tipo de Incidente	Interrupção/Falha de funções críticas
Resumo dos Eventos	Um incidente no ponto de captação Carvoeiro provoca a interrupção do abastecimento do mesmo à rede em estudo.
Extensão Geográfica	Não relevante
Duração	2 - 7 dias
Localização no tempo	Verão Não Relevante
Aviso	Longo Período de Aviso Aviso de possível interrupção do abastecimento durante um longo período de tempo.
Pessoas/Ativos em risco	A população da cidade de Aveiro. Equipamentos de ensino, justiça, governo, etc. e serviços como estabelecimentos ligados à restauração.
Informação de acontecimentos passados	Incidente imaginado, que pode afetar o sector
Causas diretas que levam à realização do cenário	☒ Fatores naturais ☒ Ações humanas intencionais ☒ Ações humanas não intencionais ☒ Defeito técnico ☒ Erros organizacionais
Informação adicional importante relativa ao cenário	

Parte 3: Análise dos Cenários de Ameaças

Cenário 6 – Falha no Carvoeiro

A: Funções críticas durante o evento

Responsabilidade de Preparação

Que funções críticas deve a organização manter e continuar se ocorrer um incidente deste tipo?

Especificar tarefas operacionais de particular importância e tarefas relacionadas com a gestão de crises para o tipo de incidente.

Descrever tarefas operacionais particularmente importantes
Ativação de reservas;

Descrever tarefas de gestão de crises
Comunicar a falha à população, incentivar a poupar água;
Organizar soluções para garantir o acesso da população a água potável.

B: Avaliação da Probabilidade

Probabilidade

Quão alta é avaliada a probabilidade de que um incidente deste tipo aconteça?

2 - Bastante Improvável

Considerar neste contexto:
Frequência: com que frequência se espera que ocorra o incidente (com base em experiências próprias ou outras, dados históricos ou estatísticos, etc.)
Plausibilidade: a possibilidade/oportunidade de que o incidente possa ocorrer (uma suposição qualificada)

Descrever os antecedentes para a avaliação da probabilidade
Não existem acontecimentos passados que permitam determinar frequência.
Considera-se que existem medidas de segurança e planos de contingência que garantem o abastecimento.

C: Avaliação de Consequências

Consequências para a organização / área de responsabilidade particular

Quais as consequências do incidente para a organização/área de responsabilidade?

Edifícios e instalações importantes	Ativação de instalações fora de serviço	1 - Limitado
Pessoal e Gestão	A gestão é afetada pois tem que arranjar soluções que permitam garantir o abastecimento à população	2 - Moderado
Sistemas IT	Descrever as consequências	Não relevante
Fornecimento de Energia	Descrever as consequências	Nível de Consequência
Acesso a materiais, bens e serviços essenciais	Interrompido o acesso ao fornecimento que abastece a rede em estudo.	4 - Severo
Transporte e Distribuição	Descrever as consequências	Não relevante
Informação e Comunicação	Descrever as consequências	Não relevante
Outros	Descrever as consequências	Nível de Consequência

Avaliação global das consequências para a organização/área de responsabilidade

Que consequências coletivas teria o incidente na continuação das funções críticas da organização? — 4 - Severo

Inserir comentários

Consequências para a sociedade em geral

Que consequências existem, diretas e/ou derivadas, devido ao incidente para a sociedade em geral?

Perda de vida e saúde	Depende da duração da interrupção do abastecimento	Nível de Consequência
Perda de Ativos (materiais, financeiros, ambientais, etc.)	Depende da duração da interrupção do abastecimento	Nível de Consequência
Ansiedade, insegurança, ira, indignação ou implicações políticas	Depende da duração da interrupção do abastecimento	Nível de Consequência
Interrupção de Infraestruturas Críticas (energia, água, transportes, etc.)	Interrupção do abastecimento de água	5 - Crítico

Avaliação global das consequências para a sociedade em geral

Que consequências coletivas, diretas e/ou derivadas do incidente podem afetar a sociedade no geral? — 5 - Crítico

Inserir comentários

Avaliação geral de consequências

Especificar o nível de consequência máximo dos pontos 4 e 6. — 5 - Crítico

D: Nível de Risco

Nível de risco para o cenário de ameaça

Cálculo do nível de risco geral baseado na probabilidade 2 - Bastante Improvável **X consequência** 5 - Crítico 10 - Risco médio

E: Avaliação de Vulnerabilidade

Preparações (antes do incidente)

Como é que a empresa se preparou, através de planeamento, etc., para gerir o incidente?

Considerar particularmente os seguintes pontos (selecionar as caixas apropriadas):

☒ Plano de preparação geral;
☐ Planos detalhados (Planos contingência, planos de segurança, etc.);
☐ Estratégia para comunicação de crises;
☐ Exercícios;
☐ Legislação, instruções, guias, etc.;
☐ Análises, avaliações de incidentes anteriores, etc.;
☐ Educação de pessoal relevante à gestão de crises;
☐ Análises de risco e vulnerabilidade anteriores;
☐ Acordos de colaboração, contratos, etc.;
☐ Outros.

Descrever as preparações

Na presente análise que não existe preparação através de planeamento

Que medidas a empresa implementou para prevenir o acontecimento do acidente ou limitar os estragos?

Considerar particularmente, se medidas foram implementadas para proteger os seguintes:

☐ Edifícios e instalações importantes;
☐ Pessoal e gestão;
☐ Sistemas IT;
☐ Fornecimento de energia;
☐ Acesso a materiais, bens e serviços essenciais;
☐ Transporte/Distribuição;
☐ Informação e comunicação
☐ Outros.

Descrever as medidas preventivas ou de mitigação dos estragos

Reservas existentes na rede

Avaliação geral das preparações

Como se avaliam as preparações da empresa para o incidente? 4 - Muitas carências

Inserir observações

Capacidades de Resposta e Alívio (durante o incidente)

Que capacidades existem à disposição para esforços de resposta e alívio se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Avaliação geral das capacidades de resposta e alívio

Como se avaliam as capacidades existentes de resposta e alívio do incidente? 5 - Altamente inadequado

Inserir observações

Capacidades de recuperação (após o incidente)

Que capacidades existem à disposição para recuperar a longo termo se o incidente ocorrer?

As capacidades podem incluir gestão, pessoal, equipamento, organização, logística, inventários, financiamento, etc.

Descrever as capacidades de resposta e alívio

Avaliação geral das capacidades de recuperação

Como se avaliam as capacidades existentes de recuperação após a ocorrência do incidente? 2 - Predominantemente adequado, poucas falhas

Inserir observações

Parte 4: Perfil de risco e vulnerabilidade

A: Delineamento

1. **O perfil de risco e vulnerabilidade foi preparado por:**

Manuela Borges

2. **A análise cobre as seguintes funções críticas:**

Abastecimento de água potável

3. **Precedentes para a análise:**

Nova análise

Catálogo de Ameaças

Categoria/Tipo de Ameaça	Exemplos
Fenómeno natural extremo	
Ameaças atmosféricas	Furacão, ciclone, tornado, tempestade de neve, inverno gelado, gelo envidraçado, nevoeiro denso, nuvens, tempestades de granizo, raios
Ameaças geológicas	Terramoto, erupção vulcânica, avalanche, deslizamento de terra
Ameaças oceanográficas	Tsunami, tempestade, inundações, gelo marinho
Terrorismo	
Ações terroristas no estrangeiro	Armas convencionais, armas CBRN, terrorismo cibernético
Acidentes de transporte (acidente, naufrágio, incêndio, explosão)	
Mar	Navios de passageiros, a granel, contentores e tanques, navios militares
Ar	Aviões de passageiros, aviões de carga, aviões militares
Caminhos de ferro	Comboios de passageiros, comboios de mercadorias
Estrada	Automóveis, autocarro, camiões
Acidentes ou emissões de substâncias perigosas / poluentes	
Substâncias químicas	Produtos químicos, gás, petróleo e derivados, gasolina, toxinas
Substâncias biológicas	Bactérias, vírus, toxinas
Substâncias radiológicas e nucleares	Radiação radioativa
Explosões	Explosões, fogo de artifício, munições
Fogos e Explosões	
Edifícios / áreas com muitas pessoas	Edifícios altos, shopping, teatros, cinemas, discotecas, estúdios, centros de conferências, hotéis, lares de idosos, hospitais, prisões, instituições, escritórios, festivais, mercados
Indústria (produção, distribuição, armazenamento, etc.)	Operações ambientalmente perigosas, armazenamento de substâncias inflamáveis / explosivas
Infraestrutura	Estações ferroviárias, aeroportos, túneis, portos
Campo	Florestas, campos
Ativos Culturais	Castelos, museus, prédios preservados, igrejas, centros históricos
Doenças e Epidemias	
Doença Humana	Bactérias, vírus, venenos
Doença do gado	Bactérias, vírus, venenos
Doenças vegetais	Bactérias, vírus, venenos

Categoria/Tipo de Ameaça	Exemplos
Destruição, interrupção ou outra falha das funções críticas da sociedade	
Energia	Eletricidade, gás, petróleo e gasolina
Comunicação e TI	Telefone fixo, telefone móvel, processamento de dados e transmissão de dados, redes de informação, acesso à internet, transmissão de TV, satélite e rádio, navegação, serviços de correio e correio
Transporte	Gestão, monitorização e controlo do tráfego de pessoal e do transporte de mercadorias (rodoviário, ferroviário, aéreo e marítimo). Vigilância e controle de infraestrutura (pontes, túneis, aeroportos, estações, portos, etc.)
Finanças e Economia	Pagamentos e transferências de dinheiro, operações bancárias e de seguros, valores mobiliários, funções do banco central
Produtos Alimentares	Abastecimento de alimentos, monitorização da segurança alimentar, monitorização de gado infecioso
Água	Abastecimento de água potável, transporte e tratamento de águas residuais
Substâncias perigosas	Controle da produção, armazenamento e transporte de substâncias perigosas (químicas, biológicas, radiológicas e nucleares)
Preparação	Alarmes e advertências, tarefas policiais, combate a incêndios, operações de resgate (terra / mar / ar), evacuação (incluindo receção, acomodação e restauração), tarefas pré-hospitalares, preparação química, preparação biológica, preparação radiológica, preparação nuclear, limpeza de munições, Preparo de tempestade, preparação ambiental, ajuda militar para autoridades civis
Saúde	Serviços de saúde primários, serviços hospitalares, cuidados de pessoas vulneráveis, monitorização de doenças infeciosas, preparação de medicamentos, produção de medicamentos
Administração pública	Capacidade de gestão de crises, manter e exercer a autoridade pelo parlamento, o governo e a administração central, os tribunais e os municípios
Segurança nacional	Guarda e vigilância de pontos-chave e fronteiras, defesa militar e execução de soberania, tarefas de inteligência, antiterrorismo, serviços de guarda-costas

Categoria/Tipo de Ameaça	Exemplos
Outras ameaças	
Crime	Ataque de TI, vandalismo / sabotagem, espionagem industrial, sequestro de resgate, chantagem, assassinato, agressão
Agitação civil	Distúrbios / repartição da ordem pública, demonstrações em larga escala, greves ou bloqueios, movimentos súbitos e maciços de pessoas
Emissão de substâncias perigosas na proximidade do seu país	Acidentes com reator nuclear ou emissões químicas no exterior
Colapsos	Grandes edifícios, estádios, pontes, infraestrutura de tráfego
Colisões	Satélites, meteoros

Anexo E - Exemplos planos a desenvolver

Exemplo de Plano de Contingência (Vieira *et al.*, 2006)

Plano de Contingência

Capítulo I - Aspectos gerais

1. Objectivos e abrangência do Plano de Contingência
2. Índice
3. Data da última revisão
4. Informação geral sobre o sistema de abastecimento
   a. Designação do sistema de abastecimento
   b. Entidade gestora
   c. Elemento(s) de contacto para o desenvolvimento e manutenção do Plano
   d. Telefone, fax e endereço electrónico do(s) elemento(s) de contacto

Capítulo II - Planos de emergência

1. Ocorrência
2. Resposta inicial
   g. Procedimentos para notificações internas e externas
   h. Estabelecimento de um sistema de gestão de emergências
   i. Procedimentos para avaliação preliminar da situação
   j. Procedimentos para estabelecimento de objectivos e prioridades de resposta a incidentes específicos
   k. Procedimentos para a implementação do plano de acção
   l. Procedimentos para a mobilização de recursos
3. Continuidade da resposta
4. Acções de encerramento e acompanhamento

Capítulo III – Anexos de suporte

Anexo 1. Informação sobre o sistema de abastecimento e localização física
   a. Mapas do sistema de abastecimento
   b. Esquemas de funcionamento
   c. Descrição das instalações/*layout*

Anexo 2. Notificação
   a. Notificações internas
   b. Notificações à comunidade
   c. Notificações a entidades oficiais

Anexo 3. Sistema de gestão da resposta
   a. Generalidades
   b. Cadeia de comando
   c. Operações
   d. Planeamento
   e. Instruções de segurança
   f. Plano de evacuação
   g. Logística
   h. Finanças

Anexo 4. Documentação de incidentes

Anexo 5. Formação e simulações em contexto real

Anexo 6. Análise crítica, revisão do Plano e alterações

Anexo 7. Análise de conformidade

Exemplo de Estrutura de Plano de Emergência (PMC, 2007)

1. Identificação do Estabelecimento/Organização

2. Características do Espaço Físico

2.1. Localização Geográfica (Anexo 2 – mapa de localização)

2.2. Distância e tempo da unidade de socorro

2.3. Descrição das instalações

2.4. População

2.5. Horário de Ocupação

3. Acesos ao edifício

3.1. Acessos ao edifício a partir do exterior

3.2. Pontos de encontro em situação de emergência

4. Identificação e localização de fontes de energia

5. Identificação dos Meios de Segurança Existentes

5.1. Equipamentos de 1ª Intervenção

5.2. Sistemas automáticos de deteção de incêndio

5.3. Extinção automática de incêndios e temperatura

5.4. Meios de alarme

5.5. Meio de alerta

6. Identificação de riscos e vulnerabilidades

6.1. Riscos internos

6.2. Riscos externos

6.3. Vulnerabilidades

7. Plano de evacuação

7.1. Procedimentos de evacuação

8. Planos de Ação

8.1. Instruções específicas

8.1.1. Responsável pela segurança

8.1.2. Alarme e alerta

8.1.3. Corte de energia

8.1.4. Primeira intervenção

8.1.5. Evacuação

8.1.6. Informação e vigilância/Concentração e controlo

8.2. Relacionamento com a comunidade e meios de comunicação social

8.3. Cooperação com autoridades

9. Informações de segurança e emergência

9.1. Antes da ocorrência

9.2. Se detetar uma ocorrência

9.3. Se ouvir o sinal de alarme

9.4. Exercícios e treinos

9.5. Revisão e atualização do plano

9.6. Autoridades